

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa



وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجنت
القلعة

MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention d'un Master académique en

« Gouvernement électronique »

Gouvernance de l'identité numérique
Cas: l'Autorité Gouvernementale de Certification
Electronique

Elaboré par:

BOUDJEMANE Noumaira

MEDJDOUB Issra

Encadré par:

Mr. DERRAR Hacene

Mr. HAMDOUN Youcef

Année Universitaire 2023/2024

RÉSUMÉ

Ce mémoire examine la gouvernance de l'identité numérique dans le cadre de la e-gouvernance en Algérie, en mettant en lumière son impact sur la modernisation des services publics. L'étude vise à comprendre les implications de l'identité numérique, analyser les défis et opportunités liés à sa gestion, évaluer les politiques existantes en matière de transparence et sécurité, et proposer des recommandations pour renforcer la protection des données et la confiance des citoyens. Basée sur une recherche documentaire, des observations et des entretiens, elle révèle que la gouvernance de l'identité numérique est essentielle pour moderniser les services publics et développer un système sécurisé et fiable. Les résultats mettent en avant les bonnes pratiques tout en identifiant les défis de sécurité, avec pour objectif d'améliorer la transparence, la sécurité et la confiance dans la gouvernance électronique en Algérie.

Mots clés : identité numérique, gouvernance électronique, transparence, sécurité, modernisation, protection des données, confiance des citoyens.

ABSTRACT

This thesis examines the governance of digital identity within the framework of e-governance in Algeria, highlighting its impact on the modernization of public services. The study aims to understand the implications of digital identity, analyze the challenges and opportunities associated with its management, assess existing policies on transparency and security, and propose recommendations to enhance data protection and citizen trust. Based on documentary research, observations, and interviews, it reveals that digital identity governance is crucial for modernizing public services and developing a secure and reliable system. The findings emphasize best practices while identifying security challenges, with the goal of improving transparency, security, and trust in electronic governance in Algeria.

Keywords: Digital identity, e-governance, transparency, security, modernization, data protection, citizen trust.

الملخص

تناول هذا البحث حوكمة الهوية الرقمية في إطار الحوكمة الإلكترونية في الجزائر، مسلطاً الضوء على تأثيرها على تحديث الخدمات العامة. تهدف الدراسة إلى فهم تأثيرات الهوية الرقمية، وتحليل التحديات والفرص المرتبطة بإدارتها، وتقييم السياسات الحالية المتعلقة بالشفافية والأمن، وتقديم توصيات لتعزيز حماية البيانات وثقة المواطنين. وباعتماد على البحث الوثائقي والملاحظات والمقابلات، تكشف الدراسة أن حوكمة الهوية الرقمية تُعد أمراً جوهرياً لتحديث الخدمات العامة وتطوير نظام أمن وموثوق. تسلط النتائج الضوء على أفضل الممارسات مع تحديد التحديات الأمنية، بهدف تحسين الشفافية والأمن وبناء الثقة في الحوكمة الإلكترونية في الجزائر.

الكلمات المفتاحية: الهوية الرقمية، الحوكمة الإلكترونية، الشفافية، الأمن، التحديث، حماية البيانات، ثقة المواطنين.

REMERCIEMENT

Tout d'abord, nous remercions Dieu le tout-puissant pour nous avoir accordé la force et la détermination nécessaires pour achever ce travail.

Nous souhaitons également remercier chaleureusement le personnel de l'Autorité Gouvernementale de Certification Électronique, en particulier M. HAMDOUD Youcef et M. HAMICH Rabah, pour leur disponibilité et leur expertise inestimable. Leur soutien a grandement facilité notre recherche et nous avons permis de mieux comprendre les enjeux complexes de la gouvernance de l'identité numérique.

Un remerciement tout particulier à notre encadrant, M. DERRAR Hacene, pour ses conseils avisés. Ses remarques constructives ont été essentielles pour la qualité de ce travail.

Enfin, nous ne pourrions conclure ces remerciements sans mentionner l'amour et le soutien indéfectible de nos familles. Leur encouragement constant et leur compréhension nous ont permis d'avancer sereinement dans cette aventure académique

Table des matières

RÉSUMÉ-----	I
ABSTRACT -----	I
المخلص-----	II
REMERCIEMENT -----	III
LISTE DES ABRÉVIATION -----	VII
LISTE DES TABLEAUX -----	X
LISTE DES FIGURES -----	XI
INTRODUCTION GÉNÉRALE -----	1
CHAPITRE I: LE CADRE THEORIQUE -----	5
Section 1: La revue de littérature. -----	6
1.1 De l'e- gouvernement a la e-gouvernance -----	6
1.2 Présentation du contexte actuel de la gouvernance électronique en Algérie. -----	11
1.3 La gouvernance a l'ère du la transformation numérique -----	12
1.4Transformation numérique en Algérie : Vers un nouveau mode de gouvernance -----	14
1.5 Présentation des initiatives précédentes liées à l'identité numérique. -----	15
1.5.1Génétique de l'identité numérique -----	15
1.5.2Anthentification transparente dans un environnement numérique ubiquitaire-----	15
1.5.3Protocoles cryptographiques pour le respect de la vie privée -----	15
1.5.4La confiance numérique dans le domaine bancaire -----	15
1.5.6L'identité numérique : une condition pour la citoyenneté numérique. -----	16
1.5.7La gestion de l'identité numérique dans les administrations publiques -----	16
1.5.8 En Afrique, l'identité numérique au service des citoyens : enjeux et défis -----	16
1.5.9L'identité numérique, clé de la confiance -----	17
1.5.10Vie privée et sécurité - Education à la citoyenneté numérique (ECN) -----	17
1.5.11La CNIBE : une technologie inexploitée -----	18
1.5.12Identité numérique sécurisée-----	18
1.5.13Protocoles cryptographiques pour le respect de la vie privée-----	18
1.5.14E-Réputation : des modèles théoriques aux méthodes de mesure -----	18
1.5.15La législation de l'identité numérique-----	19
1.6Contexte et Objectifs -----	19

1.7Résumé de la thèse sur l'identité numérique de la personne humaine -----	21
Section 2: Cadre conceptuel -----	22
2.1Les définitions -----	22
2.1.1La gouvernance :-----	22
2.1.2De e-administration á la e-gouvernance : -----	24
2.1.3 Définition de l'e-gouvernance :-----	26
2.1.4La gouvernance et l'e-gouvernance -----	27
2.1.5Transformation numérique -----	28
1.2 L'identité numérique-----	29
2.2.1Définition -----	30
2.2.2 Les acteurs de l'écosystème technique relatifs aux identités numériques -----	32
2.2.3Explication de schéma (Figure 1) les rôles définis spécifiquement par l'écosystème du règlement eIDAS 1. -----	38
2.2.4 Les normes et le cadre légale d'identité numérique : -----	40
2.3QUELQUES EXEMPLES D'IDENTITÉ NUMÉRIQUE RÉGALIEENNE DANS L'UNION EUROPÉENNE-----	45
CHAPITREII: CADRE METHODOLOGIQUE-----	46
Section 01: Introduction à la recherche qualitative -----	48
1.1Définition générale d'une étude qualitative -----	48
1.2Instruments de collecte d'information :-----	49
1.2.1. La recherche documentaire -----	49
1.2.2. L'observation-----	49
1.2.3. L'entretien -----	50
Section 02: La présentation de l'organe (Autorité Gouvernementale de Certification Electronique) -----	52
2.1Historique -----	52
2.2 Produites -----	54
2.2.1. Certificats Électronique :-----	54
2.2.2 La signature électronique -----	57
2.3Solution et services :-----	58
CHAPITRE III: RESULTATS ET DISSCUSSION -----	65
Section 01: Analyse et discussion des resultats-----	67

1.1Présentation d’entretien -----	67
1.2Analyse des résultats-----	67
1.2.1 E-gouvernance-----	68
1.2.2 Identité Numérique et E-gouvernance -----	68
1.2.3Bonnes Pratiques et Normes -----	68
1.3Discussion des résultats -----	69
1.3.1Cohérence Thématique-----	69
Section 02: Recommandation -----	70
2.1Renforcement de l'Interopérabilité des Systèmes-----	70
2.1.1Recommandation :-----	70
2.1.2 Justification :-----	70
2.2Amélioration de la Sécurité et de l'Authentification -----	70
2.2.1Recommandation:-----	70
2.2.2Justification : -----	70
2.3Mise en Œuvre d'un Cadre Réglementaire Clair et Uniforme -----	70
2.3.1Recommandation:-----	70
2.3.2 Justification: -----	71
2.4Sensibilisation et Formation des Utilisateurs -----	71
2.4.1Recommandation :-----	71
2.4.2Justification : -----	71
2.5Évaluation Continue et Adaptation des Objectifs -----	71
2.5.2Recommandation :-----	71
2.5.3Justification : -----	71
2.6Promotion de l'Innovation et de la Recherche -----	71
2.6.1Recommandation :-----	71
2.6.2Justification : -----	72
Conclusion :-----	73
CONCLUSION GÉNÉRAL-----	74
Bibliographie -----	77
ANNEXES-----	79

LISTE DES ABRÉVIATION

AECE	Autorité Économique de Certification Électronique	
AGCE	Autorité Gouvernementale de Certification Electronique	
ANCE	Autorité Nationale de Certification Électronique	
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	
API	Application Programming Interface	Interface de Programmation d'Applications
ARPCE	l'Autorité de Régulation de la Poste et des Communications Électronique	
ASP	Active Server Pages	Pages de Serveur Actives
CA	Administrateurs en chef	
CC	Certificate Chain	Chaîne de Certification
CIO	Chief Information Officer	Directeur des Systèmes d'Information
CNIBE	Carte Nationale d'Identité Biométrique Électronique	
CNIe	Carte Nationale d'Identité électronique	
CNIL	Commission Nationale de l'Informatique et des Libertés	
COE	Conseil de l'Europe	
CPS	Certificate Practice Statement	Déclaration des Pratiques de Certification
CRASC	Centre de Recherche en Anthropologie Sociale et Culturelle	

CRL	Certificate Revocation List	Liste de Révocation des Certificats
EAL4+	Evaluation Assurance Level 4+	Niveau d'Assurance d'Évaluation 4+
ECDSA	Elliptic Curve Digital Signature Algorithm	Algorithme de Signature Numérique à Courbe Elliptique
ECN	- Education à la Citoyenneté Numérique	
EDI	Échange de Données Informatisée	
EGDI	Electronic Government Development Index	Indice de Développement de l'Administration Électronique
e-Gouvernance	Gouvernance Électronique	
eID	Identification électronique	
eIDAS	electronic IDentification, Authentication and trust Services	Services d'Identification, d'Authentification et de Confiance Électroniques
ESea	e-Sécurité	e-Sécurité
HCI	Indice de Capital Humain	
IA	Intelligence Artificielle	
INE	Identifiant National Étudiant	
IoT	Internet of Things	Internet des Objets
MFA	Authentification Multi-Facteurs	
MIE	Moyen d'Identification Electronique	
NFC	Near Field Communication	Communication en Champ Proche
OCDE	l'Organisation de Coopération et de Développement Economiques	
OCSP	Online Certificate Status Protocol	Protocole de Vérification du Statut des Certificats en Ligne
ONU	Organisation des Nations Unies	

OSI	Online Service Index	Indice des Services en Ligne
OV	Organisation Validation	Validation de l'Organisation
PHP	Hypertext Preprocessor	Préprocesseur Hypertexte
PKI	Public Key Infrastructure	Infrastructure à Clé Publique
QSCD	Qualified Signature Creation Device	Dispositif de Création de Signature Qualifiée
RGPD	Règlement Général sur la Protection des Données	
RSA	Rivest-Shamir-Adleman (cryptographie)	Algorithme de Chiffrement Rivest-Shamir-Adleman
SaaS	Software as a Service	Logiciel en tant que Service
SSL	Secure Sockets Layer	Couche de Sockets Sécurisée
TIC	Technologies de l'Information et des Communications	
TII	l'Indice des Infrastructures de Télécommunications	
TSL	Transport Layer Security	Sécurité de la Couche de Transport
UE	Union Européenne	
UIT	Union Internationale des Télécommunications	
UNDESA	United Nations Department of Economic and Social Affairs	Département des Affaires Économiques et Sociales des Nations Unies
UNESCO	l'Organisation des Nations Unies pour l'éducation, la Science et la Culture	
Web RA	Registration Authority for the Web	Autorité d'Enregistrement pour le Web
ZOPE	Z Object Publishing Environment	Environnement de Publication d'Objets Z

LISTE DES TABLEAUX

Tableau 1: Les niveau de fiabilité qui doivent requis avec l'eIDAS selon le site de MANDIL AVOCATS	41
Tableau 2: Les différents types de services de confiance reconnus	43
Tableau 3: les caractéristiques des trois types d'entretiens	51
Tableau 4: Tableau d'Axe d'Entretien	67

LISTE DES FIGURES

<i>Figure 1 : Les principaux acteurs de l'ensemble de l'écosystème technique relatif aux identités numériques : un exemple d'interactions.</i>	37
<i>Figure 2: schématisations de la VIRTUAL ID de l'AGCE .</i>	59
<i>Figure 3: schématisation de Web RA de l'AGCE .</i>	61

INTRODUCTION GÉNÉRALE

À l'ère du numérique, l'identité numérique est fondamentale pour les interactions entre les individus, les entreprises et les gouvernements. Il représente toute information permettant de vous identifier clairement dans un environnement en ligne, facilitant ainsi l'accès à divers services et ressources. Pour les gouvernements, gérer efficacement cette identité numérique constitue un défi et est essentiel pour moderniser l'administration publique et renforcer la sécurité des transactions électroniques.

En Algérie, l'établissement d'une identité numérique fiable et sécurisée transformera la relation entre les citoyens et l'État en facilitant l'accès aux services publics, en améliorant l'efficacité administrative et en renforçant la confiance dans les institutions. Toutefois, cela nécessite une approche réfléchie et coordonnée qui implique un large éventail de parties prenantes, notamment les gouvernements, les entreprises technologiques, les experts en sécurité et le public lui-même. Et doté d'une identité numérique robuste, il a le potentiel de transformer fondamentalement le paysage administratif et économique.

L'expérience d'autres pays montre que l'identité numérique peut être un puissant catalyseur de développement économique et social, facilitant l'accès aux services bancaires, aux soins de santé, à l'éducation et à bien d'autres domaines. Cependant, cette transformation doit se faire avec une attention particulière aux aspects de sécurité et de protection des données afin de prévenir les risques d'abus et de cybercriminalité.

Cette étude vise à étudier différents aspects de la gouvernance de l'identité numérique, en s'appuyant sur une revue de la littérature existante, une étude de cas internationale et une analyse des particularités algériennes. Il met en évidence les meilleures pratiques, les défis à surmonter et les opportunités à exploiter pour construire un système d'identité numérique fiable et complet en Algérie. L'objectif ultime est d'élaborer des recommandations concrètes pour guider les autorités algériennes dans la mise en œuvre et la gestion des identités numériques, en veillant à ce que ce système serve les intérêts de tous les citoyens et renforce la gouvernance du pays.

Les objectifs de l'étude

Les objectifs de ce travail s'articulent sur les trois points ci-dessous :

1. Comprendre comment l'identité numérique influence les processus de gouvernance

électronique.

2. Analyser les défis et les opportunités liés à la gestion de l'identité numérique dans le contexte de la e-gouvernance.

3. Évaluer l'efficacité des politiques et des technologies d'identité numérique dans la promotion de la transparence et de la sécurité des services gouvernementaux en ligne.

4. Proposer des recommandations pour renforcer la protection des données personnelles et améliorer la confiance des citoyens dans les services publics numériques.

5. Explorer les implications éthiques et juridiques de l'identité numérique dans le domaine de la gouvernance électronique.

La problématique

Dans le but d'atteindre ces objectifs, et de tout ce qui précède, nous formulons la problématique de recherche suivante : « quel est l'impact de l'identité sur la e-gouvernance ? »

Les sous-questions

Il nous paraît important de découler une série d'interrogation afin de toucher les points suivants :

1. Comment l'adoption d'une identité numérique permettent-ils de réaliser une Bonne gouvernance ?

2. Quels sont les principaux défis liés à la protection de l'identité numérique dans le contexte de l'e-gouvernance?

3. Comment l'authentification numérique impacte-t-elle la transparence et la confiance dans les services gouvernementaux en ligne?

4. Comment les normes et réglementations en matière d'identité numérique influencent-elles la gouvernance électronique?

La méthodologie de recherche

Afin de répondre à cette problématique, nous élaborons une étude qualitative basée sur la recherche documentaire, l'observation et les entretiens adressés tant à la structure chargée de la gestion du « **Autorité Gouvernemental de Certification Electronique** » qu'à ses

acteurs et intervenants.

Ce mémoire se répartit en trois chapitres, dans le premier chapitre nous allons présenter une revue de littérature qui représente une recension des écrits ou de la documentation. Ensuite nous abordons le cadre conceptuel où nous allons définir chaque concept étudié avec les éléments clés qui l'entourent, à comprendre : « la gouvernance », « l'identité numérique ».

Dans le second chapitre, en premier temps nous allons présenter l'organisme d'accueil de « L'Autorité gouvernementale du Certification Electronique », puis nous allons aborder la méthodologie de recherche que nous avons choisie pour notre étude, tel que l'approche méthodologique retenue ainsi que l'outil de collecte de données choisit. Dans le troisième et dernier chapitre, nous allons aborder les résultats obtenus, ensuite nous allons présenter et analyser des résultats obtenus, puis nous allons procéder à la discussion de ces résultats, Enfin nous allons présenter des propositions d'amélioration, et finalement nous allons finir avec une conclusion générale.

L'objectif de l'étude

Cette étude intègre les connaissances en matière de gouvernance et de gestion d'identité numérique dans le contexte de la numérisation du secteur public, contribuant ainsi à améliorer la compréhension du concept identité numérique dans le cadre de la gouvernance. En décrivant et en analysant les pratiques liées à la gouvernance des projets, cette étude fournit des implications pour les gestionnaires et les praticiens travaillant sur le terrain

CHAPITRE I: LE CADRE THEORIQUE

Ce chapitre contient deux sections, la première traitant d'un regard sur des études antérieures liées au sujet de la recherche (la revue de littérature), tandis que la deuxième section contient un cadre théorique général sur les éléments du sujet de recherche (le cadre conceptuel).

Section 1: La revue de littérature.

Les principaux titres sur lesquels nous nous sommes concentrés dans cette section afin de présenter des sujets antérieurs liés au thème de notre recherche sont comme suite :

1.1 De l'e- gouvernement a la e-gouvernance

Le concept de gouvernance électronique a émergé en réponse aux efforts de nombreux pays pour moderniser leurs administrations publiques face au mécontentement croissant des citoyens. Ce désenchantement se manifeste notamment par la baisse des taux de participation aux élections et le sentiment que les services publics sont insuffisants et de mauvaise qualité. Une conséquence possible de cette désaffection est que les catégories les plus favorisées se détournent du système public pour se tourner vers des services privés dans des domaines comme l'éducation et la santé, ce qui peut fragmenter le consensus social autour de ces services.

Bien que les gouvernements aient utilisé les technologies de l'information et des communications (TIC) pendant plusieurs décennies et que des technologies telles qu'Internet et le Web aient été développées grâce à des fonds publics et des institutions gouvernementales, le concept de gouvernance électronique est relativement récent. Selon Oakley (2002), au Royaume-Uni, cette notion a émergé dans le cadre des efforts de modernisation entrepris par le gouvernement travailliste élu en 1997.

Cette « modernisation » était étroitement liée à ce que l'on a parfois appelé le gouvernement « interconnecté ». Les objectifs étaient double : d'une part, reconstruire les administrations publiques au service des citoyens plutôt que des producteurs, en se concentrant davantage sur les besoins des individus et la « vie réelle » ; d'autre part, reconnaître que de nombreux problèmes sociaux, tels que la criminalité et l'échec scolaire, sont liés à des interactions complexes.

Pour mieux les traiter, il était nécessaire de comprendre ces interdépendances en interconnectant les informations disponibles. Par exemple, en identifiant les élèves qui sèchent

les cours, on pourrait anticiper et prévenir des comportements déviants, grâce à une gestion intégrée des informations sur les citoyens, rendue possible par l'avènement des TIC.

Dans cette section, nous analyserons les différents modèles de gouvernance électronique en développement à travers le monde et comment ils répondent aux besoins et aspirations des citoyens dans divers contextes. Nous proposerons également quelques réflexions sur un modèle potentiel de e-gouvernance.

Les modèles de gouvernement électronique varient considérablement selon les régions et les contextes, tout comme les approches de gouvernance peuvent différer d'un endroit à l'autre. En Australie, en France, en Belgique, en Malaisie, et même à des niveaux locaux comme au cœur de Paris ou dans des zones rurales françaises, la conception de la gouvernance électronique n'est pas uniforme. Actuellement, on peut identifier trois principaux modèles de gouvernement électronique :

A. Le modèle de la « nouvelle économie » : Ce modèle met en avant les similitudes entre le gouvernement électronique et le commerce électronique. Il privilégie la fourniture de services publics de haute qualité et encourage une approche centrée sur le « self-service », avec l'objectif de réduire la taille de l'État au fil du temps. La gouvernance électronique y est perçue comme une réponse aux attentes des entreprises et des citoyens habitués aux services en ligne, en mettant l'accent sur la commodité et l'accès continu. En outre, ce modèle considère la gouvernance électronique comme un levier pour le développement économique régional et local, attirant des entreprises technologiques vers des environnements favorables à la technologie. Cependant, le développement des infrastructures suit souvent les dynamiques du marché, créant ainsi un « fossé numérique ». Les États-Unis illustrent bien ce modèle, bien que le Royaume-Uni en adopte certains aspects.

B. Le modèle de la « communauté électronique » : Préféré par des pays d'Europe continentale comme les Pays-Bas ou les nations scandinaves, ce modèle se distingue par une forte tradition de société civile et de liberté de l'information. Il met l'accent sur l'accès du public et les réseaux civils, et les interventions publiques visent à réduire les disparités numériques. Ce modèle valorise les innovations sociales issues d'un accès élargi aux technologies et voit les citoyens comme des coproducteurs des services.

C. Le modèle de l'économie planifiée : Appliqué dans des pays comme Singapour ou la Malaisie, ce modèle est caractérisé par une forte intervention du secteur public dans la direction et l'orientation des activités privées. Comme dans le modèle de la « nouvelle économie », le développement économique est crucial, mais l'État assume également la responsabilité de la construction des infrastructures et du développement des compétences nécessaires, en subventionnant largement ces initiatives.

Bien que ces modèles soient variés, ils présentent tous des limites potentielles. Le modèle de la « nouvelle économie » peut ne pas répondre aux besoins des citoyens à faibles revenus, le modèle de la « communauté électronique » favorise certaines communautés au détriment d'autres, et le modèle de l'économie planifiée peut apparaître paternaliste.

Pour concevoir un modèle efficace de gouvernement électronique, il est nécessaire de considérer la e-gouvernance comme un ensemble complexe de processus administratifs et politiques impliquant divers acteurs, tels que les secteurs public, privé et non-gouvernemental, et reliant les niveaux local, régional, national et global. Les dimensions à étudier incluent le public cible, la portée et les fonctions du système, nécessitant une analyse approfondie par des spécialistes de la sociologie, de l'économie et de la politique.

Une stratégie réussie en e-gouvernance doit inclure une volonté politique claire, un engagement civique, une accessibilité égale, des compétences adéquates, des infrastructures robustes, ainsi qu'une sécurité informatique et des considérations juridiques appropriées. Une vision globale et une stratégie à moyen et long terme sont essentielles, et il est crucial d'identifier et de répondre aux attentes des utilisateurs tout en mesurant leur satisfaction. L'investissement dans des ressources financières et humaines suffisantes est également vital pour le développement de projets de e-gouvernement.

Les technologies doivent être choisies pour leur pérennité et leur coût abordable. De nombreuses expériences dans le domaine de la e-gouvernance utilisent des plateformes gratuites et open source, telles que ZOPE, qui permet des systèmes facilement paramétrables et réutilisables. Les plateformes comme ASP et PHP sont également utilisées pour développer des projets de e-gouvernement. La sélection de ces plateformes doit viser à réduire les coûts tout en assurant la réutilisabilité, l'indépendance, et la portabilité des solutions. De plus, les technologies telles que XML, qui favorisent l'interopérabilité et le stockage des informations, jouent un rôle crucial dans la structuration des systèmes de e-gouvernance modernes.

Selon intitulé de “ digitalisation et Gouvernement électronique dans les pays du Maghreb : états des lieux et perspectives ” qui a été présenter un état de lieux d’Alger . l’Algérie a lancé un programme ambitieux intitulé « E-Algérie 2013 » dans le but de renforcer les performances de son économie, de ses entreprises et de son administration. Adoptée par le gouvernement en janvier 2009, cette stratégie vise à faire émerger une société algérienne du savoir et de la connaissance, tout en développant des clusters industriels dans les technologies de l’information et de la communication (TIC). Un état des lieux initial a permis de définir des objectifs majeurs et spécifiques pour la période 2009-2013, accompagnés d’un ensemble d’actions nécessaires à leur réalisation.

Le plan multisectoriel « E-Algérie 2013 » a été structuré autour de plusieurs axes, d’A à M, avec la gestion confiée au ministère de la Poste et des TIC, et a bénéficié d’importants investissements publics. Le premier axe majeur de cette stratégie concerne le développement de l’administration électronique, visant à accélérer l’adoption des TIC dans les services publics par l’introduction et le renforcement de ces technologies au sein de l’administration.

Après 11 ans de mise en œuvre, plusieurs réalisations illustrent les avancées en e-administration. Parmi celles-ci:

- Le portail El-Mouatin, destiné à permettre le téléchargement de formulaires officiels et la consultation d’informations relatives à la vie quotidienne, bien qu’il ne soit pas encore indexé par les moteurs de recherche.
- L’introduction de passeports et cartes d’identité biométriques, avec un suivi en ligne des dossiers. En 2019, plus de 14 millions de passeports biométriques et 16 millions de cartes d’identité biométriques avaient été délivrés.
- En réponse aux défis sanitaires, Sonelgaz a mis en place des dispositifs de paiement en ligne pour ses clients en mars 2020, tandis qu’Algérie Poste propose également le paiement en ligne de diverses factures et la recharge de crédits téléphoniques.
- Algérie Poste a enregistré 2.417.723 transactions électroniques en huit mois en 2020, avec une forte proportion réalisée via sa propre plateforme monétique.
- Le ministère de la Justice a mis en place des services électroniques permettant la demande d’extraits de casier judiciaire et de certificats de nationalité en ligne, ainsi

qu'une plateforme de parquet électronique pour la soumission de plaintes et requêtes à distance.

- Divers autres services électroniques, tels que le retrait de documents d'état-civil à distance et la création d'une identité virtuelle pour les assurés sociaux, ont également été développés, améliorant la sécurité et la gestion des démarches administratives.

L'Algérie a d'ailleurs été reconnue pour ses avancées en matière de télé-déclaration et d'e-paiement pour les cotisations à la sécurité sociale lors de la 8ème édition du concours mondial sur la société de l'information, organisé par l'Union internationale des télécommunications.

La gouvernance électronique, ou e-gouvernance, exploite les technologies de l'information et de la communication (TIC) pour moderniser les processus internes des administrations publiques et améliorer l'efficacité des services offerts. Elle cherche également à renforcer la relation entre le gouvernement et les citoyens, en favorisant une plus grande implication dans les politiques et les processus démocratiques. Ce modèle, bien ancré dans les pratiques gouvernementales, est souvent intégré dans des programmes de réforme visant à créer des administrations plus efficaces, transparentes et orientées vers les TIC. En Asie, malgré une croissance économique notable et un développement significatif des infrastructures TIC, des défis subsistent, notamment en termes d'inégalités de revenus et de pénétration du haut débit. Cet article évalue l'état et l'évolution de l'e-gouvernance en Asie, en se basant sur des données internationales pour analyser les performances régionales, les disparités entre sous-régions, et l'impact potentiel sur la qualité de la gouvernance. Les résultats révèlent des progrès mais aussi des fractures persistantes qui nécessitent des stratégies adaptées et une meilleure coopération régionale pour combler les écarts et améliorer la gouvernance.

Évaluation de l'administration électronique en Algérie

Pour évaluer l'administration électronique, divers indicateurs ont été développés par des organisations internationales, des institutions académiques et des pays. L'évaluation la plus complète est celle effectuée par l'ONU sur l'administration électronique. Depuis 2001, le Département des affaires économiques et sociales des Nations Unies (UNDESA) publie un

rapport annuel sur l'administration électronique. Ce rapport, connu sous le nom d'EGDI (Electronic Government Development Index), mesure le développement de l'administration électronique à l'échelle nationale et sert de référence pour établir un classement des États membres des Nations Unies en matière de développement de l'administration électronique.

L'EGDI est calculé en faisant la moyenne pondérée de trois dimensions principales de l'administration en ligne :

- **L'étendue et la qualité des services en ligne**, mesurées par l'Indice de service (OSI), basé sur les données collectées par un site web indépendant.
- **L'état du développement des infrastructures de télécommunications**, évalué par l'Indice des infrastructures de télécommunications (TII), utilisant les données fournies par l'Union internationale des télécommunications (UIT).
- **Le capital humain**, mesuré par l'Indice de capital humain (HCI), dont les données proviennent principalement de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO).

1.2 Présentation du contexte actuel de la gouvernance électronique en Algérie.

Prévisions 2023 : 12 tendances en matière de gouvernance numérique et de diplomatie

La publication a été publiée le 6 janvier 2023. Révisé le 20 janvier 2024. Le document intitulé « Prévisions 2023 : 12 tendances en matière de gouvernance et de diplomatie numériques » rédigé par Jovan et la DiploTeam. Gouvernance numérique, diplomatie, normes numériques, coopération numérique. Un résumé de 12 tendances importantes en matière de gouvernance et de diplomatie numériques. Projections concernant les avancées majeures dans le domaine de la gouvernance numérique et de la diplomatie. Les progrès de la gouvernance numérique devraient s'accélérer en réponse aux tensions géopolitiques et aux problèmes sociétaux liés à la numérisation.

Les enjeux économiques de la mise en œuvre du règlement sur la gouvernance des données

En 2023, la publication intitulée « Les défis économiques de l'adoption de la réglementation sur la gouvernance des données » a été rédigée par la Commission nationale de l'informatique et des libertés. Le document traite de la réglementation de la gouvernance des données, de la loi sur la gouvernance des données, de la confiance, de l'intermédiaire de données, de la neutralité économique, des modèles économiques, de la sécurité juridique et des études économiques. Il analyse les répercussions économiques de la mise en œuvre du règlement sur la gouvernance des données en France, en mettant l'accent sur la neutralité économique et la confiance dans l'échange de données. Les défis liés à la mise en œuvre du règlement sur la gouvernance des données concernent l'établissement d'un statut d'intermédiaire de données digne de confiance afin de garantir la neutralité économique des intermédiaires. Cela implique des aspects tels que l'autonomie du modèle commercial, la flexibilité des prix et la transparence.

1.3 La gouvernance à l'ère de la transformation numérique

L'article sur Atalayar aborde les premiers pas vers la démocratie électronique, mettant en lumière l'importance de la numérisation des services publics pour moderniser l'administration et offrir des services de qualité accessibles à tous. Djaouad Allal, expert en numérisation, souligne que la numérisation va au-delà de la simple transmission de documents par e-mail, en permettant une meilleure exploitation des données et une gouvernance améliorée. Abderrahmane Hadeif, expert en économie, insiste sur la transformation numérique comme un changement socioculturel plaçant l'humain au cœur de cette évolution. L'article souligne également les progrès réalisés en Algérie depuis les premières expériences de numérisation en 2003-2004, notamment dans les secteurs de la justice et de l'intérieur, et la nécessité d'une vision globale et d'une stratégie nationale pour la numérisation du pays.

L'Algérie a franchi une nouvelle étape dans le processus de numérisation des documents administratifs et de lutte contre la bureaucratie. La numérisation fait partie du plan d'action du gouvernement pour moderniser l'administration publique et offrir des services publics de qualité accessibles à tous les citoyens. Selon Djaouad Allal, expert en numérisation, la numérisation va au-delà de scanner un document et l'envoyer par e-mail. Elle permet d'éviter l'intervention humaine pour donner un service, analyser des données, les exploiter et mieux gouverner. Pour Abderrahmane Hadeif, expert en économie, il faut parler de "transformation

numérique" car c'est une transformation socioculturelle qui place l'humain au centre. Les premières expériences de numérisation remontent à 2003-2004 au ministère de la Justice, suivi du ministère de l'Intérieur avec le passeport biométrique en 2015. Désormais, pour la première fois, les documents de citoyenneté peuvent être collectés via une plateforme numérique dédiée. Cependant, la fracture numérique reste un défi car certains citoyens n'arrivent pas à accéder ou maîtriser ces technologies. Le paradigme a changé : ce sont les services qui viennent maintenant vers les citoyens.

L'article sur Atalayar explore les premiers pas vers la démocratie électronique, mettant en avant l'importance de la numérisation des services publics pour moderniser l'administration et offrir des services de qualité accessibles à tous. Djaouad Allal, expert en numérisation, souligne que la numérisation va au-delà de la simple transmission de documents par e-mail, en permettant une meilleure exploitation des données et une gouvernance améliorée. Abderrahmane Hadeff, expert en économie, insiste sur la transformation numérique comme un changement socioculturel plaçant l'humain au cœur de cette évolution. L'article souligne également les progrès réalisés en Algérie depuis les premières expériences de numérisation en 2003-2004, notamment dans les secteurs de la justice et de l'intérieur, et la nécessité d'une vision globale et d'une stratégie nationale pour la numérisation du pays.

L'article d'El Watan sur la transformation numérique en Algérie, selon l'expert Djallal Bouabdallah : Le président Abdelmadjid Tebboune a placé la numérisation et la digitalisation au cœur du programme ambitieux du gouvernement pour moderniser l'administration publique, stimuler l'économie et renforcer la connectivité numérique sur tout le territoire. En août 2023, la création du Haut Commissariat à la numérisation souligne le rôle crucial de ce secteur dans la régulation de l'économie algérienne. Cette stratégie repose désormais sur ce haut commissariat chargé de concevoir, suivre et mettre en œuvre la stratégie nationale de numérisation des différents secteurs. Selon Djallal Bouabdallah, expert en transformation digitale, l'Algérie se positionne à un moment crucial dans son parcours de transformation digitale. Elle développe ses capacités technologiques, modernise l'administration pour une gouvernance électronique et réduit la fracture numérique. Cette transformation est cruciale pour l'avenir économique et social de l'Algérie, en lui permettant de rester compétitive dans un monde de plus en plus numérisé, tout en améliorant la qualité de vie des citoyens. Les données sont devenues des actifs stratégiques clés dans ce contexte. Les technologies comme le cloud,

l'IA, l'IoT, le Big Data et la blockchain pourraient jouer un rôle déterminant.

Voici un résumé de l'article d'El Watan sur les défis de la numérisation en Algérie : Bien que le projet "e-Algérie" lancé en 2009 et relancé en 2018 ait permis à l'Algérie de gagner des places dans le classement du e-Government Development Index des Nations Unies, passant de la 120^e à la 112^e place en 2022, le pays fait encore face à des obstacles dans la réalisation des objectifs de numérisation. Même si plus de 450 plateformes numériques ont déjà été lancées dans différents secteurs, le taux de digitalisation n'est pas encore à son plus haut niveau. Le niveau d'utilisation réelle de ces plateformes n'est pas connu. Le président Abdelmadjid Tebboune s'est plaint à plusieurs reprises des lenteurs dans le processus de numérisation. Beaucoup reste à faire pour atteindre les résultats escomptés et le niveau des autres pays de la région, malgré les efforts fournis. Le ministre des Finances, Laâziz Fayed, a insisté sur l'importance d'aller par étapes dans la numérisation de son secteur, sans précipitation. La numérisation n'est pas seulement une question de technologie, mais aussi de transformation des processus, des mentalités et de la culture. Le travail doit se faire non seulement sur les logiciels et les plateformes, mais aussi sur les hommes, car une transformation numérique impacte le pouvoir dans les structures concernées, ce qui peut susciter de la résistance au changement. En résumé, bien que des progrès aient été accomplis, la numérisation en Algérie fait encore face à des défis importants liés à l'utilisation réelle des plateformes, à la transformation des mentalités et à la résistance au changement, nécessitant une approche progressive et globale.

1.4 Transformation numérique en Algérie : Vers un nouveau mode de gouvernance

En 2023, l'article intitulé « Transformation numérique en Algérie : vers un nouveau mode de gouvernance » rédigé par Hacene Derrar et publié dans le journal El Watan explore l'importance de la transformation numérique, de la gouvernance, de la stratégie et de la politique en Algérie. L'article souligne que la transformation numérique joue un rôle crucial dans le progrès économique et social de toute nation, les autorités publiques algériennes faisant preuve d'un fort engagement en faveur de sa réussite. Néanmoins, la mise en œuvre efficace des stratégies de numérisation continue de poser des problèmes. Bien que l'article reconnaisse les progrès de la transformation numérique en Algérie, il n'aborde pas les obstacles spécifiques liés à la mise à l'échelle des initiatives d'identité numérique et à la

garantie de leur sécurité et de leur accessibilité. En outre, des obstacles persistent dans le déploiement de stratégies de numérisation complètes dans divers secteurs et dans la mise en place de plateformes numériques homogènes.

1.5 Présentation des initiatives précédentes liées à l'identité numérique.

1.5.1 Génétique de l'identité numérique

L'article « Génétique de l'identité numérique » écrit par Julien Pierre en 2011 explore l'examen des mécanismes d'identité en ligne facilités par les systèmes automatisés, mettant en lumière les conséquences socio-politiques et scientifiques associées à l'identité numérique. Pierre explore les dimensions génétiques de l'identité numérique et leurs répercussions sur la vie privée et la sphère publique.

1.5.2 Authentification transparente dans un environnement numérique ubiquitaire

En 2021, l'article « L'authentification transparente dans un environnement numérique omniprésent » rédigé par Takoua Guiga présente une nouvelle approche de l'authentification qui exploite la biométrie pour renforcer la sécurité des interactions entre les utilisateurs et les appareils interconnectés. L'objectif principal de cet article est de répondre aux préoccupations liées à la confidentialité, à la sécurité et à la convivialité dans un paysage numérique étendu.

1.5.3 Protocoles cryptographiques pour le respect de la vie privée

Neals Fournaise a été crédité comme l'auteur de l'article intitulé « Protocoles cryptographiques pour la confidentialité » en 2022. L'étude explore le domaine de la cryptographie et des techniques de cryptage, en examinant des éléments tels que la sécurité des systèmes bancaires, les mécanismes d'échange de clés et l'utilisation de signatures numériques pour garantir la confidentialité des données.

1.5.4 La confiance numérique dans le domaine bancaire

En 2022, Marine Julien a écrit un article intitulé « La confiance numérique dans le

secteur bancaire ». La présente étude explore le domaine de la confiance numérique et des cadres réglementaires au sein du secteur bancaire, en mettant en lumière des facteurs critiques tels que la protection de la confidentialité des données, la transparence et les mécanismes de sécurité régissant les transactions bancaires.

1.5.6 L'identité numérique : une condition pour la citoyenneté numérique.

En 2022, la mise en place d'une identité numérique est considérée comme essentielle pour la manifestation de la citoyenneté numérique. Rédigée par TADJEDDINE Bachir, cette notion englobe divers éléments tels que l'identité numérique, les méthodes de paiement et la sécurité personnelle. L'intégration de l'identité numérique a le potentiel d'améliorer considérablement les procédures administratives et les engagements entre les particuliers et les organismes gouvernementaux, en garantissant la protection de la vie privée et en rationalisant l'adoption des innovations en matière de paiement.

1.5.7 La gestion de l'identité numérique dans les administrations publiques

Examen de la gestion de l'identité numérique dans les administrations publiques par Betty N. Merhi Batoul publié en 2022. Ce travail scientifique explore le domaine de la gestion de l'identité numérique au sein des administrations publiques, en se concentrant sur les obstacles liés à la confidentialité, à la sécurité et au respect des lois. Il met l'accent sur les conséquences de l'essor de l'identité numérique sur les libertés individuelles, la vie privée et la dignité humaine, ainsi que sur les obstacles sociétaux liés à cette transformation.

1.5.8 En Afrique, l'identité numérique au service des citoyens : enjeux et défis

En 2023, l'utilisation de l'identité numérique au profit des citoyens en Afrique est explorée dans le texte rédigé par Camille Dubruelh. Le concept d'identité numérique joue un rôle crucial dans la mise en place de nations intelligentes en Afrique ; cependant, son accessibilité est encore limitée. L'importance de l'identité numérique pour la gouvernance et l'efficacité de la prestation de services est bien reconnue par les pays africains. Malgré des

avancées notables, l'adoption de l'identité numérique n'est pas encore inclusive, ce qui entraîne l'exclusion de certaines personnes. Pour promouvoir la mise en œuvre généralisée de l'identité numérique, les pays africains doivent concevoir des stratégies qui soutiennent l'innovation sans créer d'obstacles. Bien que l'article souligne l'importance de l'identité numérique en Afrique, il n'aborde pas les défis spécifiques qui entravent la mise en œuvre à grande échelle des identités numériques et des solutions correspondantes.

1.5.9 L'identité numérique, clé de la confiance

En 2023, un article intitulé « L'identité numérique, clé de la confiance » a été publié dans le magazine EDI, rédigé par Frédéric Bergonzoli. Des concepts tels que l'identité numérique, la confiance, le tiers de confiance, l'authentification et le certificat électronique jouent un rôle essentiel dans l'établissement de la confiance numérique, avec des professionnels certifiés par l'ANSSI et utilisant des certificats électroniques.

Le secteur de la confiance numérique a connu une croissance de plus de 10 % en 2022, tandis que la proposition d'un portefeuille d'identité numérique européen a le potentiel de renforcer la confiance entre diverses entreprises et organisations.

1.5.10 Vie privée et sécurité - Education à la citoyenneté numérique (ECN)

En 2024, l'article intitulé « Confidentialité et sécurité - Éducation à la citoyenneté numérique (ECN) » rédigé par la COE Digital Citizenship, Privacy, Security Society, souligne la nécessité d'établir une politique de confidentialité et de sécurité dans les programmes scolaires. Cette initiative vise à doter les enfants et les jeunes de compétences numériques et d'une autonomie adéquates, leur permettant d'exercer leurs droits et responsabilités en tant que citoyens actifs à l'ère d'Internet. L'importance de l'éducation à la citoyenneté numérique réside dans la protection de la vie privée et de la sécurité de tous les citoyens, en mettant particulièrement l'accent sur les jeunes, tout en encourageant une utilisation responsable d'Internet. Bien que l'article souligne le rôle essentiel de l'éducation à la citoyenneté numérique dans la protection de la vie privée en ligne, il n'aborde pas spécifiquement les obstacles pratiques liés à la mise en œuvre généralisée de l'identité numérique dans des régions comme l'Afrique et l'Algérie.

1.5.11 La CNIBE : une technologie inexploitée

En 2024, Gaan.dz a publié un article sur le CNIBE, une technologie encore inexploitée. Le CNIBE, qui englobe l'identité numérique, la biométrie et les fonctionnalités de sécurité, représente une avancée technologique sous-utilisée en Algérie. Il offre un niveau sophistiqué de sécurité physique et logique et répond à de multiples objectifs tels qu'une carte d'identité, une carte de paiement, une carte de santé, etc. L'intégration de la CNIBE en Algérie a le potentiel de rationaliser les processus administratifs et de renforcer la sécurité des transactions en ligne.

1.5.12 Identité numérique sécurisée

Au cours de l'année 2024, La publication intitulée Secure Digital Identity, rédigée par Thales Group, Le concept d'identité numérique, ainsi que ses tendances et technologies, gagnent du terrain dans divers secteurs tels que le secteur privé et les citoyens. L'évolution d'identité numérique influence profondément nos interactions avec les entités institutionnelles. Les entreprises du secteur privé participent activement à l'exploration de l'identité numérique, en introduisant de nouvelles tendances qui auront un impact significatif sur le paysage de l'identité numérique, non seulement en 2022 mais également à l'avenir.

1.5.13 Protocoles cryptographiques pour le respect de la vie privée

Neals Fournaise a été crédité comme l'auteur de l'article intitulé « Protocoles cryptographiques pour la confidentialité » en 2022. L'étude explore le domaine de la cryptographie et des techniques de cryptage, en examinant des éléments tels que la sécurité des systèmes bancaires, les mécanismes d'échange de clés et l'utilisation de signatures numériques pour garantir la confidentialité des données.

1.5.14 E-Réputation : des modèles théoriques aux méthodes de mesure

En 2021, les travaux universitaires de la chercheuse Liliane Bara ont été rendus publics sous le titre : « E-réputation : des modèles théoriques aux méthodes de mesure ». Cette étude explore le domaine de l'e-réputation en passant en revue les techniques d'audit et d'évaluation, ainsi que l'analyse des sentiments en ligne. L'étude souligne l'importance de l'utilisation d'instruments numériques pour la surveillance de la réputation en ligne des individus et des

entités.

1.5.15 La législation de l'identité numérique

Le projet de loi n° 992, déposé au Conseil National de Monaco le 12 juin 2019, vise à établir un cadre juridique pour l'identité numérique dans le contexte de l'évolution rapide des technologies numériques et de l'Internet. Voici les points clés de ce document :

1.6 Contexte et Objectifs

Le projet de loi répond à la nécessité croissante de sécuriser l'identité numérique des utilisateurs face aux risques d'usurpation et de fraude. Avec l'essor des réseaux sociaux et des services en ligne, chaque individu laisse des traces numériques qui nécessitent une réglementation pour protéger les données personnelles et garantir la confiance des utilisateurs dans les services numériques.

Les objectifs principaux de ce projet de loi incluent :

- La création d'une identité numérique monégasque unique pour chaque individu.
- L'établissement d'un registre national pour centraliser et sécuriser les données d'identification.
- La mise en place de mécanismes d'authentification fiables pour prévenir les fraudes et les usurpations d'identité.
- La reconnaissance de cette identité par les plateformes de services de confiance.

Le projet est structuré en dix articles qui définissent les termes clés et établissent les bases de l'identité numérique. Parmi les définitions importantes:

- **Identification numérique** : Processus utilisant des données personnelles sous forme électronique pour représenter de manière unique une personne.
- **Données d'identification personnelles** : Informations utilisées pour l'identification, y compris des caractéristiques physiques et biométriques.

• **Fournisseurs d'identité** : Entités responsables de la gestion et de la maintenance des données d'identification.

L'identité numérique de la personne humaine. Contribution à l'étude du droit fondamental à la protection des données à caractère personnel

La thèse intitulée « L'identité numérique de la personne humaine : Contribution à l'étude du droit fondamental à la protection des données à caractère personnel » propose une analyse approfondie de la manière dont l'identité humaine est affectée par les données numériques et comment cette réalité se reflète dans le droit à la protection des données personnelles.

La thèse aborde les difficultés liées à la définition et à la protection des données à caractère personnel, un sujet devenu crucial à l'ère numérique. Elle souligne que, malgré de nombreux efforts pour clarifier et systématiser ce concept, la législation reste imprécise et les tentatives de définition se heurtent à l'ambiguïté du texte légal. La définition légale des données personnelles est large et inclut une vaste gamme d'informations, ce qui complique leur gestion et leur protection.

L'auteur propose que la notion d'identité numérique est essentielle pour comprendre la nature des données personnelles. L'identité numérique désigne l'ensemble des informations, qu'elles soient objectives ou subjectives, relatives à une personne, qui sont numérisées par des procédés informatiques. Cette approche met en lumière que les données personnelles ne sont pas simplement des éléments d'identification mais des composantes intégrales de l'identité humaine.

La thèse examine comment le droit positif aborde les données à caractère personnel. Elle critique la tendance du droit à considérer les données personnelles comme une catégorie autonome, distincte des droits à la vie privée et à la personnalité. Cette dissociation crée une confusion et profite souvent aux responsables de traitement des données. Le droit fondamental à la protection des données personnelles apparaît ainsi comme une notion imparfaite, incapable de pleinement protéger l'individu dans le contexte numérique actuel.

L'analyse révèle que la protection des données personnelles est souvent insuffisante pour garantir la véritable autonomie de l'individu. En France et au niveau européen, les droits conférés aux individus sont souvent ponctuels et dépendent du consentement, ce qui peut être problématique face au déséquilibre de pouvoir entre les individus et les responsables du

traitement des données. La thèse critique également l'idée que la protection des données personnelles soit simplement un moyen de faciliter la circulation des données dans le marché intérieur plutôt qu'un droit fondamental réel.

La thèse suggère que pour que la protection des données personnelles devienne un droit véritablement fondamental, il est nécessaire de renforcer le concept d'identité numérique dans le cadre juridique. L'auteur appelle à une meilleure intégration de cette notion dans le droit pour garantir une protection plus cohérente et efficace de la personne humaine contre les intrusions numériques.

En conclusion La thèse conclut que l'identité numérique doit être reconnue comme un élément central dans la législation sur la protection des données personnelles. Il est crucial de développer un cadre juridique qui protège non seulement les données en tant qu'éléments isolés mais aussi l'intégrité de l'identité humaine dans le monde numérique. Cela nécessitera une révision des normes juridiques actuelles pour garantir une protection adéquate des individus dans un environnement de plus en plus dominé par les technologies numériques.

1.7 Résumé de la thèse sur l'identité numérique de la personne humaine

Cette thèse, soutenue en 2018 à l'Université Lumière-Lyon-2, étudie la notion juridique de donnée à caractère personnel et la protection des données personnelles comme droit fondamental. L'auteur suggère que l'élément clé manquant pour comprendre la nature des données personnelles est le concept d'identité numérique de la personne humaine.

Projection de l'identité dans le numérique:

- Les données personnelles sont des informations relatives à une personne qui ont fait l'objet d'une numérisation.
- L'identité de la personne humaine est l'objet des données à caractère personnel, qui intègre la dimension subjective de la personne (vécu, choix, actions).
- La prolifération des identifiants formels (nom, date de naissance, etc.) et leur mise en réseau permettent de recomposer un portrait substantiel de la personne, projetée sur les supports numériques.

Protection de l'identité dans le numérique :

- Le droit des données personnelles a une ambivalence congénitale : il garantit implicitement la liberté de collecte pour les responsables de traitement, au-delà de la protection des personnes.

- La priorité est que les données circulent avec fluidité pour libérer leur potentiel économique, la protection des personnes n'étant plus véritablement la finalité première.

- Dans ce contexte, l'encouragement à la sociabilité peut être un moyen d'orientation ou de contrôle des comportements, à l'inverse de l'autonomie de la personne.

En conclusion, la projection permanente de l'identité des personnes par numérisation appelle en théorie une réaction forte du droit pour protéger l'identité numérique de la personne humaine.

Section 2: Cadre conceptuel

Au cours de cette section nous avons abordé un cadre conceptuel dont les différents concepts clés qui sont relative à notre étude pour comprendre le problème de recherche et orienter l'investigation. De plus, il décrit les théories fondamentales, les idées et les concepts pertinents pour notre étude et explique comment l'identité numérique et la gouvernance sont liés à l'ère de la transformation numérique, aussi quel est l'impact de l'identité numérique sur la e-gouvernance en Algérie ainsi que toute interaction possible entre eux.

2.1 Les définitions

2.1.1 La gouvernance :

De l'anglais *governance*, art de gouverner indépendant de l'autorité étatique. (Soucieuse de souplesse, de transdisciplinarité et du respect des enjeux environnementaux, elle repose sur la participation de différents acteurs de la société civile). (Dictionnaire LAROUSSE).

La **gouvernance** désigne l'ensemble des mesures, des règles, des organes de décision,

d'information et de surveillance qui permettent d'assurer le **bon fonctionnement et le contrôle** d'un Etat, d'une institution ou d'une organisation qu'elle soit publique ou privée, régionale, nationale ou internationale.

Selon le dictionnaire de politique, la gouvernance a "pour but de fournir l'orientation stratégique, de s'assurer que les objectifs sont atteints, que les risques sont gérés comme il faut et que les ressources sont utilisées dans un esprit responsable". Elle veille en priorité au **respect des intérêts des "ayants droits"** (citoyens, pouvoirs publics, partenaires, actionnaires...) et à faire en sorte que leurs voix soient entendues dans la conduite des affaires.

Initialement utilisé pour désigner la manière dont un gouvernement exerce son autorité économique, politique et administrative et gère les ressources d'un pays en vue de son développement, le concept de "gouvernance" a ensuite été étendu à la **gestion des entreprises**.

Issu de la théorie micro-économique et de la science administrative anglo-saxonne, la notion de "**bonne gouvernance**" a été diffusée dans les années 1990 par la **Banque mondiale**, comme la condition nécessaire des politiques de développement.

La gouvernance repose sur **quatre principes fondamentaux** :

- la responsabilité,
- la transparence,
- l'Etat de droit,
- La participation.

Dans un sens plus étroit, la gouvernance d'entreprise correspond à l'articulation entre les actionnaires et la direction de la société, c'est-à-dire plus particulièrement au fonctionnement du conseil d'administration, directoire ou conseil de surveillance.

Les détracteurs de la gouvernance y voient une idéologie du **désengagement**, voire de **recomposition de l'État** s'inscrivant dans la vision de l'Etat minimal, depuis le tournant néolibéral des années 1980.

« La Définition de la bonne gouvernance » selon Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH)

La gouvernance fait référence à l'ensemble des processus de gouvernement, aux

institutions et aux processus et pratiques en matière de prise de décision et de réglementation concernant les questions d'intérêt commun. La bonne gouvernance ajoute une dimension normative ou une dimension d'évaluation au processus de gouvernement. Du point de vue des droits de l'homme, elle fait avant tout référence au processus par lequel les institutions publiques conduisent des affaires publiques, gèrent des ressources publiques et garantissent la réalisation des droits de l'homme.

Bien qu'il n'existe pas de définition internationalement reconnue de ce qu'on appelle la bonne gouvernance, celle-ci peut couvrir les thèmes suivants : le plein respect des droits de l'homme ; l'état de droit ; la participation effective ; les partenariats multipartites ; le pluralisme politique ; la transparence et l'application du principe de responsabilité dans les procédures et dans les activités des institutions ; l'efficacité et l'efficacé du secteur public ; la légitimité ; l'accès à la connaissance, à l'information et à l'éducation ; la disponibilité de moyens d'action politique ; l'équité ; la viabilité ; des attitudes et des valeurs qui favorisent la responsabilité, la solidarité et la tolérance.

Les piliers de la bonne gouvernance

Le Conseil des droits de l'homme a reconnu que les piliers de la bonne gouvernance étaient :

- la transparence ;
- la responsabilité ;
- L'obligation de rendre compte de ses actes ;
- la participation ;
- La capacité de répondre aux besoins de la population.

2.1.2 De e-administration à la e-gouvernance :

Au début des années 1990, l'accès du plus grand nombre à Internet a porté les administrations publiques à s'investir sur des politiques de modernisation de l'action publique qui voyaient dans le numérique des nouvelles possibilités de mise en relation avec les

citoyens. Tandis qu'en principe il s'agissait d'une démarche à but informatif et administratif, aujourd'hui les outils numériques développés par les collectivités territoriales visent à une majeure interaction, dont la modernisation des processus de participation citoyenne par l'emploi du n

L'histoire de l'emploi du numérique par l'administration publique pour la relation aux citoyens a commencé en France vers la fin des années 90. En 1997, le plan Jospin « Internet, un défi pour la France » posait un premier cadre normatif pour l'ouverture des sites Internet administratifs et le portail Admifrance en fut la première expérimentation (Bacache-Beauvallet et al, 2011). Quelques années plus tard, le gouvernement s'est investi progressivement dans la transition numérique des services publics et, au début des années 2000, service-public.fr rassemblait pour la première fois tous les services publics numériques français constitue l'un des enjeux majeurs.

Depuis, l'évolution des usages et des savoirs numériques a accompagné les politiques de modernisation pour la relation au citoyen, portant les collectivités à adapter leur action publique aux pratiques numériques. Un exemple parmi d'autres, en septembre 2014 la sixième version du site gouvernement.fr depuis son lancement en 1996 était mise en ligne, tandis que le succès des réseaux sociaux portait à une modification importante de ses fonctionnalités. Alors qu'il s'agissait principalement d'un outil d'information de la politique gouvernementale, aujourd'hui la nouvelle interface invite les usagers au *partage* des infographies et des contenus sur les réseaux sociaux, à les rendre virales par l'accompagnement d'hashtags et à consulter les contenus augmentés. De la même manière, sous l'impulsion de la croissante production de données et des politiques de transparence face aux citoyens, en 2011 le gouvernement français ouvrait son premier portail unique interministériel pour la publication des données publiques. Data.gouv.fr devient le symbole d'une ultérieure étape de la modernisation des services publics à travers l'*ouverture* des données et la *contribution* des citoyens. Aujourd'hui le portail recueille 14 740 jeux de données et la publication des données est alimentée par la participation des « internautes ».

(La construction de l'action publique dans le domaine de l'internet en France, Laurent Sorbier, P213 à 237)

2.1.3 Définition de l'e-gouvernance :

Le concept d'e-Gouvernance (Gouvernance électronique) fait référence à l'intégration des Technologies de l'Information et de la Communication (TIC) et des technologies numériques dans l'administration d'un pays. Son objectif est de soutenir et de simplifier la gouvernance pour toutes les parties : gouvernement, citoyens et entreprises, en contribuant à obtenir à terme une bonne gouvernance.

Cela implique une planification, une gestion, une coordination et une supervision efficaces de l'ensemble du processus de transformation numérique des institutions publiques. La gouvernance électronique peut améliorer la gestion et la communication des informations financières, accélérer le traitement de divers processus, réduire les coûts, améliorer la communication avec les citoyens et potentiellement servir de Catalyseur pour une plus grande responsabilisation et davantage de participation de la part des citoyens dans les processus publics.

La gouvernance électronique, ou e-gouvernance, cherche à tirer avantage des technologies de l'information et de la communication (TIC) pour transformer les processus internes des organisations publiques, et rendre leur offre de services publics plus efficace et performante. Elle vise également à améliorer les modes opératoires des relations qu'entretient le gouvernement avec les usagers (les citoyens et les entreprises en particulier), pour permettre davantage d'implication et de participation dans les politiques et les processus démocratiques. L'e-gouvernance, en tant qu'utilisation stratégique des TIC par les gouvernements, comprend donc des modes opératoires au sein de l'administration, des prestations de service public et des processus démocratiques.

L'e-gouvernance en tant que paradigme transformationnel fondé sur les TIC pour l'administration et la gestion publiques est bien établie et largement acceptée. Les initiatives transformationnelles sont en général mises en place dans le cadre d'un Programme général de réforme administrative du gouvernement. Ces programmes de réforme cherchent avant tout à former des gouvernements qui coûtent moins, offrent des services personnalisés de grande qualité, soient dotés d'une fonction publique professionnelle, puissent tirer profit des TIC de façon stratégique, aient une meilleure capacité de régulation et soient intègres et transparents dans leur mode de gouvernance.

Donc si on donne une définition identique pour la gouvernance électronique ou E-

gouvernance serait l'utilisation des TIC pour obtenir une meilleure gouvernance.

Selon la définition de l'OCDE, Le « meilleur gouvernement » c'est qui implique une plus grande efficacité et de meilleures performances de la part du gouvernement, ainsi que sa capacité à offrir des services publics de qualité ; une meilleure gouvernance inclurait également la possibilité pour les intervenants de s'engager davantage dans les politiques et les processus démocratiques.

2.1.4 La gouvernance et l'e-gouvernance

La gouvernance électronique, ou e-gouvernance, cherche à tirer avantage des technologies de l'information et de la communication (TIC) pour transformer les processus internes des organisations publiques, et rendre leur offre de services publics plus efficace et performante. Elle vise également à améliorer les modes opératoires des relations qu'entretient le gouvernement avec les usagers (les citoyens et les entreprises en particulier), pour permettre davantage d'implication et de participation dans les politiques et les processus démocratiques. L'e-gouvernance, en tant qu'utilisation stratégique des TIC par les gouvernements, comprend donc des modes opératoires au sein de l'administration, des prestations de service public et des processus démocratiques.

L'e-gouvernance en tant que paradigme transformationnel fondé sur les TIC pour l'administration et la gestion publiques est bien établie et largement acceptée. Les initiatives transformationnelles sont en général mises en place dans le cadre d'un Programme général de réforme administrative du gouvernement. Ces programmes de réforme cherchent avant tout à former des gouvernements qui coûtent moins, offrent des services personnalisés de grande qualité, soient dotés d'une fonction publique professionnelle, puissent tirer profit des TIC de façon stratégique, aient une meilleure capacité de régulation et soient intègres et transparents dans leur mode de gouvernance.

Donc si on donne une définition identique pour la gouvernance électronique ou E-gouvernance serait l'utilisation des TIC pour obtenir une meilleure gouvernance.

Selon la définition de l'OCDE, Le « meilleur gouvernement » c'est qui implique une plus grande efficacité et de meilleures performances de la part du gouvernement, ainsi que sa capacité à offrir des services publics de qualité ; une meilleure gouvernance inclurait

également la possibilité pour les intervenants de s'engager davantage dans les politiques et les processus démocratiques.

Des modèles de maturité pour l'e-gouvernance, variés mais très similaires, ont été proposés par les organisations internationales telles que le Département des affaires économiques et sociales des Nations Unies UNDESA et l'OCDE.

Ces modèles définissent quatre étapes majeures dans la maturité des e-gouvernements : information, interaction, transaction, transformation.

Les stratégies d'e-gouvernement guident la transition des pays au cours des différentes étapes de maturité. Ces stratégies se concentrent sur trois zones principales de développement : infrastructure, intégration et transformation.

Les stratégies orientées vers l'infrastructure s'intéressent à la création d'infrastructures de l'information à la fois au sein du gouvernement et dans la société – dont les connections Internet abordables pour les citoyens font partie.

Les stratégies orientées vers l'intégration s'intéressent à la façon dont le développement des infrastructures peut être utilisé pour le partage des informations, et à la façon dont les services publics peuvent être mieux délivrés par des systèmes de package et d'intégration, à partir de modèles de gouvernance centrés sur les citoyens et les entreprises.

Les stratégies de transformation précisent la façon dont les services peuvent innover, grâce à des modèles de gouvernance en réseaux et des pratiques de gestion des connaissances.

On résume que la différence entre ce deux termes E-gouvernance et la gouvernance réside dans l'intégration des TIC dans la stratégie de la gouvernance.

2.1.5 Transformation numérique

La « transformation digitale » est évoquée dans des contextes de plus en plus nombreux et elle est souvent associée à des termes aussi barbares que vagues, généralement des anglicismes : blog, e-learning, analytics, hashtag, MOOC, Natives, Crowdfunding, Cloud, Big Data, Blockchain, ... Par conséquent, l'expression est aujourd'hui parfois galvaudée et il est difficile de comprendre exactement à quoi l'on se réfère. Il nous a donc semblé important, dès la première question de cet ouvrage, de clarifier ce point et de donner une définition claire de ce que nous entendons par « Transformation digitale ». L'e-gouvernement

De nombreuses définitions du gouvernement électronique ont été formulées par des chercheurs et de grandes organisations internationales. L'une des plus simples et certainement des plus complètes est offerte par l'Organisation de coopération et de développement économiques (OCDE). Elle définit l'e-gouvernement comme l'utilisation des TIC pour obtenir un meilleur gouvernement. (E-Government Studies, OCDE, 2003)

L'utilisation des technologies de l'information et des communications (TIC) dans les administrations publiques, associée à des changements au niveau de l'organisation et de nouvelles aptitudes du personnel. L'objectif est d'améliorer les services publics, renforcer les processus démocratiques et de soutien aux politiques publiques. (La définition d'E-gouvernement par la communauté européenne)

De nombreuses définitions du gouvernement électronique ont été formulées par des chercheurs et de grandes organisations internationales. L'une des plus simples et certainement des plus complètes est offerte par l'Organisation de coopération et de développement économiques (OCDE). Elle définit l'e-gouvernement comme l'utilisation des TIC pour obtenir un meilleur gouvernement.

L'e-gouvernance et l'e-gouvernement sont deux concepts interconnectés qui se réfèrent à l'utilisation des technologies de l'information et de la communication (TIC) pour améliorer les services publics et la gestion gouvernementale. Voici une analyse détaillée de ces deux notions.

1.2 L'identité numérique

Avec l'essor des outils numériques, les utilisateurs génèrent une quantité considérable de données personnelles, que ce soit de manière intentionnelle ou involontaire. Cela inclut des actions comme l'achat de produits sur des sites de commerce en ligne, l'utilisation de services de géolocalisation, l'échange d'emails, le remplissage de formulaires en ligne, et l'interaction sur les réseaux sociaux. Chacune de ces activités laisse des traces numériques, sur lesquelles l'utilisateur a un contrôle variable. Ces données permettent de créer un profil personnel, constituant ainsi une « identité numérique ».

Dans ce titre nous allons aborder les pointes essentielles liées à l'identité numérique, on rependard aux questions suivants :

-C'est quoi une identité numérique ?

- Quel est l'écosystème d'une identité numérique ?
- Quel sont les technologies pour une identité numérique fiable ?
- Quels sont les normes et le cadre légale d'identité numérique ?

2.2.1 Définition

L'identité numérique : de quoi parle –t-on?

D'après le dossier de la Commission nationale d'informatique et liberté sur l'identité numérique :

Dans le domaine de la sécurité des informations, et plus généralement dans celui des systèmes informatiques, l'identité est un ensemble d'éléments liés à une personne physique qui permet de la connecter à d'autres informations.

Ces caractéristiques sont des traits propres à la personne dans un environnement spécifique. Par nature, ils sont divers. Les noms, prénoms, adresses, empreintes digitales et signature vocale sont parmi ceux qui sont plutôt stables dans le temps. Certains changent fréquemment, tels que la localisation géographique ou la tenue vestimentaire.

La notion d'identité numérique est utilisée lorsque ces caractéristiques sont enregistrées pour être utilisées en ligne, notamment pour interagir avec des systèmes d'information.

Une identité numérique est basée sur un dispositif d'identification électronique (ou MIE), c'est-à-dire un objet matériel et/ou immatériel qui contient des informations d'identification personnelle et qui sert à s'authentifier à un service en ligne. Le MIE peut se présenter sous la forme d'une application sur un smartphone, d'une carte à puce ou d'un compte en ligne.

Il y a différentes identités numériques pour une même personne, car chaque identité varie en fonction du contexte et du niveau de garantie de sa fiabilité (attribut déclaré, choisi ou vérifié avec un niveau de vérification spécifique).

Une identité en ligne permet de développer une certaine confiance en ligne pour :

L'identification est une méthode permettant de différencier une personne d'une autre au sein d'une population spécifique, comme l'utilisation d'identifiants nationaux tels que le numéro national étudiant (INE).

L'authentification consiste à démontrer que l'individu est bien une de ses identités, par

exemple en fournissant le mot de passe correspondant à un identifiant ; La démonstration de caractéristiques d'identité : qui permet de prouver des éléments de son identité (tels qu'une nationalité, un statut d'étudiant, un âge ou le fait d'être majeur). La plupart des systèmes d'information utilisent les données d'identité afin de gérer au moins les utilisateurs, les administrateurs et les personnes impliquées dans les traitements de ce système. Plus précisément, la gestion des identités dans ces traitements est associée aux questions de politique d'habilitation, d'exactitude des données ou d'exercice des droits. La CNIL ne s'intéresse cependant pas ici à la question de l'identité numérique dans ces situations. Son attention se porte sur l'utilisation de l'identité numérique dans le cadre de schémas d'identification tels que ceux définis par le règlement européen eIDAS ou qui permettent son utilisation dans divers systèmes, conformément aux normes établies. (DOSSIER THÉMATIQUE L'identité numérique,

Selon TADJEDINE El Bachir, l'identité numérique peut être définie comme suit :

La question de l'identité, en tant que droit inhérent aux individus ayant principalement la nationalité algérienne, mérite d'être abordée. La gestion de l'identité, la tenue des registres d'état civil, l'octroi de la nationalité et la délivrance des cartes d'identité nationales sont des responsabilités de l'État.

La détention d'un certificat de naissance ou d'une carte d'identité nationale donne au titulaire le statut de citoyen et lui donne la possibilité de participer à des activités civiles, d'être inscrit dans des établissements d'enseignement, de participer à des processus démocratiques, d'accéder à la protection sociale, de créer des entreprises commerciales, d'ouvrir des comptes bancaires, d'obtenir une assurance, etc.

Quand quelqu'un se rend à l'administration pour effectuer des transactions officielles, il doit d'abord s'identifier en répondant à la question « Qui -vous ? » Ensuite, l'individu fait une vérification de son identité en présentant sa carte d'identité nationale afin de confirmer son identité affirmée. Le personnel administratif doit s'assurer que la photo sur la pièce d'identité est identique à celle de la personne debout devant lui, en mettant en évidence l'importance d'une présence physique.

La digitalisation des procédures administratives permet aux citoyens de réaliser des tâches officielles en ligne grâce à des dispositifs électroniques. Cependant, cette dématérialisation pose un nouveau défi pour l'État : comment vérifier et authentifier les

utilisateurs en ligne qui n'ont plus besoin de se rendre physiquement dans les bureaux administratifs ? Ce dilemme est résolu par la création de systèmes d'identité numérique. « L'identité numérique offre à chaque individu la possibilité de prouver facilement, de manière sécurisée et sans ambiguïté son identité en ligne afin d'accéder à des services en ligne. »

2.2.2 Les acteurs de l'écosystème technique relatifs aux identités numériques

Nous nous appuyons ici sur les divers acteurs impliqués dans l'identité numérique et sa construction ainsi que sur le déroulement de l'opération. Les protagonistes majeurs de tout le système technique lié aux identités numériques Selon notre ouvrage *Identités numériques* (2016), l'écosystème technique des identités numériques en France, en Europe et à l'échelle mondiale repose principalement sur le triangle « utilisateurs (3.2.1), fournisseurs de services électroniques (3.2.4), niveaux de confiance ». Depuis, cet écosystème a connu une grande complexification, en particulier en ce qui concerne les niveaux de confiance, qu'il s'agisse des fournisseurs d'identité numérique (3.2.2), des autorités de délivrance de l'identité primaire (3.2). .3) ou des fournisseurs d'attributs (3.2.5).

De leur côté, les acteurs industriels ont mis à jour leur offre (3.2.6). L'objectif que nous visons ici est de présenter l'organisation fondamentale de cet écosystème et de saisir le rôle joué par ces six catégories d'acteurs, sans prétendre à l'ensemble.

- Les utilisateurs (« users »)

L'utilisateur est défini comme la personne ou la société, ou la personne représentant une personne physique ou morale, qui possède l'identité numérique. Un ensemble de données est utilisé pour identifier ou authentifier l'utilisateur en ligne ou hors ligne, ainsi que pour gérer les attributs et les justificatifs liés à son identité numérique. La déclaration d'identité d'un utilisateur (nom, prénom, pseudonyme, adresse e-mail) est un signe d'identification. Lorsqu'un utilisateur fournit des informations qui prouvent son identité (comme un mot de passe envoyé par SMS), il s'authentifie.

C'est donc un individu qui possède un moyen numérique (smartphone, ordinateur, tablette...) pour gérer ses informations d'identification (nom de famille, prénom, date de naissance, lieu de naissance, adresse actuelle, sexe, adresse de courrier électronique...), ses caractéristiques (couleur des yeux, statut vaccinal, photographies de l'utilisateur, données biométriques...), ses justificatifs (permis de conduire, diplôme, attestation de vaccination...) liés à son identité numérique.

Il peut aussi s'agir d'une entité juridique, c'est-à-dire d'un ensemble ayant la personnalité juridique, qui, par le biais d'une personne physique, s'identifie ou s'authentifie en ligne ou hors ligne, fournit des caractéristiques (immatriculation au Registre du Commerce et des Sociétés) ou des supports (déclaration d'imposition) liés à son identité numérique.

- Les fournisseurs d'identités numériques (digital identity providers)

Le prestataire d'identité numérique est une entité publique ou privée qui offre à l'utilisateur une identité en ligne. Il est possible que cette identité numérique soit émise par l'autorité de délivrance de l'identité originelle.

Le fournisseur d'identité numérique remplit sa fonction minimale en enregistrant l'utilisateur ; il gère les informations d'identification et d'authentification pour une authentification en ligne. (Décret n° 2022-676 du 26 avril 2022 qui permet la mise en place d'un dispositif d'identification électronique appelé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 qui permet la mise en place d'un dispositif d'identification électronique appelé « Authentification en ligne »).

- Les autorités de délivrance de l'identité primaire

Un organisme public, l'autorité de délivrance de l'identité primaire, assure la fiabilité du lien initial entre la personne physique ou morale et l'identité électronique ou numérique qui lui est attribuée sur un support physique et/ou logiciel. Ce gouvernement délivre une carte d'identité ou un titre d'identité (carte nationale d'identité, passeport, titre de séjour). Différentes informations d'identification peuvent être incluses dans ces identités primaires (données d'état civil, données appelées « pivot »).

L'autorité qui fournit l'identité primaire est déterminée par le degré de garantie et de sécurité du service demandé par le service électronique qui nécessite l'authentification de l'utilisateur. L'utilisateur utilise une identité numérique fournie par une autorité de délivrance de référence pour payer ses impôts, car il a besoin d'un service électronique correspondant au niveau de garantie attendu.

L'utilisateur utilise une identité numérique fournie par une autorité de délivrance de référence pour payer ses impôts, car il a besoin d'un service électronique correspondant au niveau de garantie attendu. L'autorité qui fournit l'identité primaire est déterminée par le degré de garantie et de sécurité du service demandé par le service électronique qui nécessite l'authentification de l'utilisateur. (La partie de confiance ministère d'intérieure).

- Les fournisseurs de services électroniques (electronic service providers)

Le prestataire de services électroniques offre un service électronique public ou privé qui donne à l'utilisateur la possibilité d'accéder à des ressources ou de réaliser des actions en ligne ou hors ligne. En conséquence, le prestataire de services a la possibilité d'identifier et/ou d'authentifier l'utilisateur, c'est-à-dire de garantir qu'il s'agit de la personne appropriée en faisant appel, généralement, à un niveau de confiance.

Un grand nombre de services électroniques sont offerts par les fournisseurs de services électroniques.

Par exemple, l'assurance maladie, Pôle emploi et la peuvent offrir des services électroniques publics pour suivre l'avancement du traitement d'une demande. Ils proposent diverses actions, telles que l'accès aux documents administratifs (comme le certificat de naissance), la déclaration et le paiement des impôts, la démarche pour obtenir un permis de conduire, l'accès à son dossier médical partagé et la possibilité de bénéficier d'offres de soins. Impots.gouv.fr est à la fois un service électronique et un service d'identification numérique.

Il est possible de se baser sur l'identification/authentification électronique de l'utilisateur, qu'il effectue lui-même ou qui est effectué par un autre service de l'État via FranceConnect. (FranceConnect est basé sur une association d'identités, qui assure la mise en place d'un système de connexion entre les identités d'un utilisateur dans divers systèmes d'information).

Les opérateurs de télécommunications, les plateformes d'achat en ligne et les banques peuvent offrir des services électroniques privés. Dans cette situation, le prestataire de services électroniques détermine ou authentifie l'utilisateur en se référant notamment à :

- Une identité numérique qui peut être consultée à partir d'un document physique (carte nationale d'identité électronique, passeport électronique, titre de séjour électronique) délivré par une autorité primordiale de délivrance d'identité.

Une identité numérique fournie par un prestataire d'identité numérique (améli.fr, impots.gouv.fr) ou une identité fournie par des organismes publics, Mobile Connect et moi ou YRIS fournis par des

organismes privés).

- Une méthode d'authentification électronique enregistrée auprès de la Commission européenne en respectant les règles du règlement eIDAS 1 (comme L'Identité Numérique La Poste).

- Les fournisseurs de justificatifs ou de données (credentials and data providers)

Les prestataires de justificatifs ou de données (fournisseurs de certificats et de données) Le prestataire de preuves ou de données recueillies, élabore et transmet des caractéristiques d'une personne et/ou des attestations d'attributs. À la demande de l'utilisateur, il communique avec le prestataire de services électroniques et le prestataire d'identité numérique. Le prestataire de documents ou de données a la possibilité de recueillir directement des attributs ou de les générer à partir de documents tels qu'un diplôme, un permis de conduire, un certificat d'état civil, une facture d'électricité. En 2016, nous avons indiqué qu'il était un acteur optionnel.

-Les acteurs industriels

Nous distinguons ici deux types d'acteurs industriels :

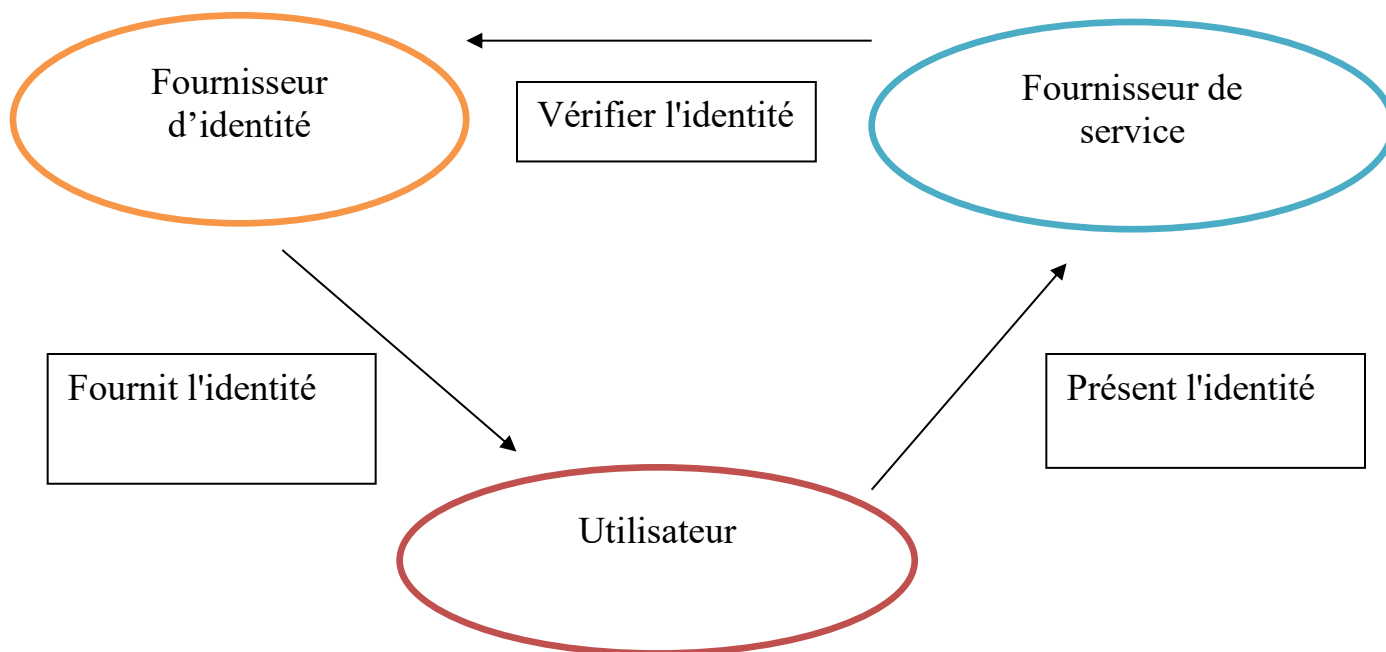
A/Les acteurs industriels du marché des identités offrent des solutions matérielles et/ou logicielles :Des solutions matérielles et/ou logicielles sont proposées par les acteurs industriels du marché des identités, telles qu'une carte à puce, un élément sécurisé dans un smartphone, une puce NFC intégrée au smartphone permettant de lire les données enregistrées dans la carte à puce . à une carte d'identité, ou bien de communiquer hors ligne des éléments d'identités virtuelles avec des systèmes de vérification d'identités. Ces intervenants satisfont directement les besoins des autorités chargées de la délivrance de l'identité primaire, des fournisseurs d'identités numériques, des prestataires de services et des fournisseurs de documents justificatifs ou de données.(NFC pour Near Field Communication ou Communication en champ proche d'une dizaine de centimètres).

B/Les acteurs industriels fournissant l'infrastructure technique des identités sous-jacente mettent en œuvre :Les fournisseurs d'infrastructure technique des identités sous-jacentes sont responsables de la mise en place, de l'exploitation et de la maintenance de tous

les moyens informatiques mis en place. Leur mais est de s'assurer que l'infrastructure sous-jacente est disponible et fiable pour tous les acteurs de l'écosystème. Les fournisseurs de services de cloud ou les fournisseurs de blockchain, ainsi que les concepteurs et administrateurs d'interfaces de programmation ou d'Application Programming Interface (API) font partie de cette catégorie.

Il est important de se rappeler que les fabricants de smartphones proposent à leurs utilisateurs, grâce à leur banque d'applications mobiles, des applications qui gèrent les portefeuilles d'identité numérique.

Figure 1 : Les principaux acteurs de l'ensemble de l'écosystème technique relatif aux identités numériques : un exemple d'interactions.



Source : Elaboré par nous-même selon le dossier numérique de l'identité numérique de la CNIL.

D'après les informations fournies par la concernant l'identité numérique, un système d'identification qui permet à une personne d'utiliser son identité numérique implique au moins trois acteurs :

Un utilisateur : un individu désireux d'accéder à divers services en ligne et hors ligne ;

Un prestataire d'identité : un tiers de confiance qui fournira un MIE. Il est par défaut responsable des attributs présentés par l'utilisateur et du lien entre ces attributs et cet utilisateur. Cependant, il peut également faire appel à des fournisseurs d'attributs afin d'ajouter des caractéristiques au MIE tout en assurant la qualité ;

Un prestataire de services : une entreprise publique ou privée qui offre à l'utilisateur un ensemble de services dont l'accès est soumis soit à une authentification, soit à une preuve d'attribut(s). Chaque MIE offre un niveau de garantie spécifique en fonction du contexte d'utilisation, allant d'une identité déclarative (par exemple, une identité sur un réseau social basée sur un pseudonyme ou un nom d'usage choisi par l'utilisateur sans vérification) à une

identité régalienne, c'est-à-dire garantie par l'État (par exemple, l'identité numérique associée à la nouvelle carte nationale d'identité électronique (CNIe).

2.2.3 Explication de schéma (Figure 1) les rôles définis spécifiquement par l'écosystème du règlement eIDAS 1.

Pour garantir la reconnaissance mutuelle entre les individus et les entreprises, le règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur adopté et ses mesures d'exécution établissent un cadre commun pour les interactions électroniques de « confiance ». Les utilisateurs sont inclus dans ce socle, ainsi que les entités qui fournissent les moyens d'identification électronique, les entités chargées de l'enregistrement des données d'identification personnelle uniques, les parties utilisatrices, les prestataires de services "considérés comme" de confiance.

- **Le concept d'utilisateurs** : L'utilisateur n'est pas défini dans le règlement. Selon le règlement, l'utilisateur fait appel à des méthodes d'identification électronique attestées par un État membre de l'UE et/ou à des services de confiance réglementés par le règlement. Selon eIDAS 1, l'utilisateur représente une partie des utilisateurs.

- **Les entités qui délivrent les moyens d'identification électronique (issuers of electronic identification means)** Les fournisseurs de moyens d'identification électronique (fournisseurs de moyens d'identification électronique) utilise une fois le terme « entités qui fournissent les moyens d'identification électronique », sans donner de définition. Dans la version anglaise du règlement, ce mot est traduit par « émetteurs de moyens d'identification électronique notifiés », une expression qui peut également être traduite par « émetteurs de moyens d'identification électronique notifiés ».

« L'identification électronique » est définie comme « l'utilisation de données d'identification personnelle sous forme électronique d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ».

L'identification électronique est définie comme « un dispositif matériel et/ou immatériel qui contient des informations d'identification personnelle et qui sert à s'authentifier pour un service en ligne ».

Un fournisseur d'identité numérique est une entité qui fournit un moyen d'identification

électronique, comme défini dans le point 1.4 de ce document. Les utilisateurs peuvent bénéficier d'un logiciel ou d'une application mobile pour s'authentifier auprès des "parties utilisatrices".

L'identification électronique peut se faire à l'aide d'un élément matériel (carte d'identité électronique ou passeport électronique équipé d'une puce) ou d'une application mobile. Trois niveaux de garantie peuvent être appliqués, le cadre se distinguant :

- Le faible niveau de garantie vise à diminuer le risque d'utilisation abusive de l'identité revendiquée, par exemple en se référant à un seul élément d'authentification tel qu'un mot de passe ;

Le niveau de protection « important » vise à diminuer considérablement le risque d'utilisation abusive de l'identité en ajoutant un autre facteur d'authentification au mot de passe préalablement entré, comme un code temporaire envoyé par SMS.

- Le niveau de protection « élevé » vise à prévenir l'utilisation abusive de l'identité en remplissant les exigences du niveau substantiel, en particulier en mettant en place des mesures de protection « contre les attaquants à haut potentiel d'attaque ». Selon le règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015, les niveaux de garantie des moyens d'identification électronique mentionnés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques sont définis. Le titre d'identité électronique est utilisé en France pour confirmer une authentification de garantie élevée.

Il est également stipulé que « les moyens d'identification électronique pertinents du schéma d'identification électronique » sont fournis : i) Par l'État membre qui notifie ce schéma d'identification électronique à la Commission européenne (ci -après « État membre notifiant »), ii) Dans le cadre d'un mandat de l'État membre notifiant, ou

iii) Quelle que soit la notification de l'État membre et leur reconnaissance par cet État membre.

2.2.4 Les normes et le cadre légale d'identité numérique :

- Règlement Général sur la Protection des Données (RGPD)

Le RGPD, mis en place en mai 2018, renforce la sécurité des informations personnelles en Europe. Il impose des exigences rigoureuses aux entreprises en ce qui concerne la collecte, le traitement et la conservation des informations personnelles, tout en accordant aux individus un plus grand pouvoir de contrôle sur leurs données.

Le règlement général de l'UE (Union européenne) sur la protection des données (RGPD) établit les règles concernant le traitement et le transfert des données personnelles des individus dans l'UE.

Qu'est-ce que le RGPD?

La législation la plus rigoureuse au monde en matière de protection de la vie privée et de sécurité est le règlement général de l'UE (l'Union européenne) sur la protection des données. Les principes énoncés dans la directive de 1995 sur la protection des données ont été actualisés et modernisés par ce règlement. Il a été approuvé en 2016 et a été mis en vigueur le 25 mai 2018.

Le RGPD définit les termes suivants :

- Les droits essentiels des individus à l'ère du numérique
- Les responsabilités de ceux qui gèrent les informations
- Les moyens de garantir le respect des règles
- Les punitions envers ceux qui ne se conforment pas aux règles.

2.2.4.1 Conditions de reconnaissance mutuelle des moyens d'Eid

Afin d'être reconnu dans tous les pays de l'UE (une exigence depuis le 29 septembre 2018), un moyen d'eID doit répondre aux critères suivants : • Donner la possibilité d'accéder à au moins un service public en ligne de l'Union européenne.

Tableau 1: Les niveau de fiabilité qui doivent requis avec l'eIDAS selon le site de MANDIL AVOCATS

Garantie	Fiabilité	Objectif
FAIBLE	Accorde un degré limité de fiabilité de l'identité revendiquée ou prétendue d'une personne	Réduire le risque d'utilisation abusive ou d'altération de l'identité
SUBSTANTIELLE	Accorde un degré substantiel de fiabilité de l'identité revendiquée ou prétendue d'une personne	Réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité
ELEVÉE	Accorde un degré de fiabilité plus élevé	Empêcher l'utilisation abusive ou l'altération de l'identité

L'évaluation du niveau de garantie est basée sur la fiabilité que le moyen d'eID correspond à l'identité revendiquée ou prétendue d'un individu. Il est essentiel de procéder à l'attribution de ces niveaux en respectant les spécifications, normes et procédures minimales établies par le règlement d'exécution n°2015/1502 du 8 septembre 2015. Les niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 est défini par le règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015.

Il prend en considération les critères de preuve et de vérification d'identité (authenticité des documents d'identité présentés, comparaison des caractéristiques physiques du demandeur...).

Par exemple, le niveau bas requiert l'utilisation d'au moins un des trois éléments d'authentification : la possession, la connaissance et l'incohérence. Les niveaux importants et élevés requièrent deux personnes. Cependant, le règlement ne précise aucun moyen technique ou organisationnel et ne favorise aucune technologie supplémentaire. Il a pour objectif de donner aux États la possibilité de préserver leur souveraineté nationale dans certains domaines de la sécurité informatique tels que la cryptographie, tout en favorisant l'innovation technologique grâce à des solutions nationales afin de répondre aux exigences du règlement. Plus précisément, il n'est pas nécessaire de se rencontrer en personne (c'est-à-dire entre le demandeur de l'identification et la

personne qui fournit le moyen d'identification).

- Avoir été remis en accord avec un schéma communiqué par l'État membre concerné à la Commission européenne et figurer sur la liste publiée par la Commission au JOUE.

Il est nécessaire que les autres États membres reçoivent la description du schéma six mois au moins avant la notification .

L'État membre a la possibilité de notifier un schéma entièrement ou en partie. On peut obtenir le moyen d'eID soit par l'État membre lui-même, soit par un acteur privé reconnu par l'État. Seules l'Allemagne et l'Italie ont déjà envoyé à la Commission un schéma d'identification pour le moment. Il est prévu que la France suive rapidement avec le système d'identité numérique développé par France Connect, qui est le point de connexion entre les eID et les fournisseurs de services des autres États membres.

2.2.4.2 Les services de confiance numérique :

Les exigences techniques sont établies dans le règlement pour les services de confiance qui sont généralement fournis au public contre rémunération et qui ont des conséquences sur des niveaux.

Ce règlement ne s'applique pas à :

- la prestation de services exclusivement utilisés dans des systèmes fermés au sein d'un groupe spécifique de participants, ce qui les rend inopposables aux tiers, comme les systèmes mis en place par des entreprises ou des administrations publiques pour gérer les procédures internes ou un système d'identification entre une banque et ses clients.
- les questions liées à la rédaction et à la validité des contrats ou autres obligations juridiques lorsqu'il y a des exigences formelles imposées par le droit national ou de l'UE. Il est possible que les parties soient impliquées dans une transaction dérogeant éventuellement aux dispositions du règlement.

2.2.4.3 Les différents types de services

Il s'agit de cinq services de confiance qui permettent à chacun deux ou trois niveaux de confiance. Les États peuvent utiliser ces services et établir d'autres formes de services de confiance reconnues à l'échelle nationale.

Tableau 2: Les différents types de services de confiance reconnus

Services	Niveaux de confiance		
Signature électronique (Personne physique)	SIMPLE	AVANCÉE	QUALIFIÉE : reconnue et acceptée dans tous les états membres
Cachet électronique (Personne morale)			
Horodatage électronique	SIMPLE (garantie de non-répudiation)	QUALIFIÉ : reconnue et acceptée dans tous les états membres : le service bénéficie d'effets juridiques identiques au même service ramené au papier, lorsqu'il existe	
Service d'envoi recommandé électronique	SIMPLE	QUALIFIÉ : le service bénéficie d'effets juridiques identiques au même service ramené au papier, lorsqu'il existe	
Authentification de sites internet			

Elaboré par l'eIDAS selon le site de MANDIL AVOCATS .

2.2.4.4 Les Obligations et responsabilités des prestataires de services de confiance

Deux catégories de prestataires sont distinguées par le règlement : le prestataire non qualifié et le prestataire qualifié.

Dans les deux situations, il est essentiel que le fournisseur prenne les mesures appropriées afin de gérer les risques liés à la sécurité. Plus précisément, il est tenu de signaler toute violation de la sécurité ou de perte d'intégrité « qui a un impact significatif sur le service de confiance offert ou sur les données personnelles qui y sont stockées ». Il est nécessaire de notifier dans un délai de 24 heures l'organe de contrôle (en France, l'ANSSI) et, le cas échéant, les autres organismes concernés (organisme national compétent en matière de sécurité de l'information, autorité chargée de la protection des données, etc.) ainsi que les personnes bénéficiant du service de confiance et susceptibles de subir un préjudice.

- Le prestataire compétent est confronté à des exigences s'accumulent : Être inscrit sur les listes de confiance nationales (celle de l'ANSSI en France). Les listes de confiance visées à l'article 22, 5 du règlement (UE) no 910/2014 sont définies par la décision d'exécution (UE) 2015/1505 de la Commission du 8 sept. 2015.

- examinateur attentivement tous les éléments particuliers de la personne physique ou morale auxquels il délivre le certificat qualifié .
- Maintenir une base de données sur les certificats à jour et fournir des informations précontractuelles à ses clients ;
- profiter d'une assurance responsabilité appropriée ;
- garantir la pérennité du service ;
- adopter des mesures adéquates concernant les preuves à présenter en justice ;
- transmettre, au minimum tous les deux ans, un rapport d'audit à l'ANSSI ;

Selon les principes de non-discrimination et de neutralité technologique, la qualification n'est pas un critère pour l'efficacité juridique et la recevabilité d'une signature, d'un cachet, d'un horodatage ou d'un envoi électronique recommandé comme preuves en justice.

Des services non qualifiés peuvent être utilisés et ne peuvent pas être refusés comme preuves. Toutefois, l'interopérabilité diminue. Par ailleurs, l'utilisateur n'a pas une présomption « légale » de fiabilité. En effet, si les fournisseurs de services de confiance sont tenus responsables des préjudices causés intentionnellement ou par négligence à une personne en raison d'un non-respect de leurs obligations, la responsabilité de la preuve est différente :

- Le prestataire qualifié est considéré comme responsable, à moins qu'il ne démontre que les dommages ont été causés sans intention ni négligence de sa part ;
- En revanche, l'utilisateur qui invoque l'existence d'un préjudice doit prouver la faute du prestataire non qualifié.

Du côté du prestataire qualifié, la qualification constitue la reconnaissance d'un niveau « élevé » de fiabilité technique. L'objectif est qu'elle soit perçue comme un signe de confiance qui prendra la forme d'un label mis en œuvre par la Commission européenne.

Selon le fournisseur qualifié, la qualification représente la preuve d'un niveau « élevé » de technicité. Il est important qu'elle soit perçue comme un signe de confiance qui se traduira par un label établi par la Commission.

2.3 QUELQUES EXEMPLES D'IDENTITÉ NUMÉRIQUE RÉGALIENNE DANS L'UNION EUROPÉENNE

En Estonie, une identité numérique certifiée existe depuis 2002 grâce à une carte nationale d'identité électronique qui est un document d'identité obligatoire. Cette carte contient une puce sécurisée où sont insérés deux certificats, l'un pour l'authentification en ligne, l'autre pour la signature électronique.

En Allemagne, une carte d'identité électronique a été créée en 2010. Si l'utilisation de cette carte est obligatoire, la fonction d'identité numérique régaliennne qu'elle offre aux citoyens allemands a été facultative et laissée à la main de l'utilisateur jusqu'en 2017.

En Belgique, dès 2004, une carte d'identité électronique obligatoire a été délivrée à chaque citoyen. En cinq ans, la Belgique est parvenue à doter 100 % de sa population de ce nouvel outil, qui contient une puce intégrant deux certificats : l'un permettant l'authentification en ligne, l'autre permettant l'apposition de la signature électronique de son détenteur

La notification consiste en la reconnaissance mutuelle d'un schéma d'identification électronique d'un État membre par les autres États membres. Cette identité numérique peut alors être utilisée dans toute l'Union européenne.

CHAPITRE II: CADRE METHODOLOGIQUE

Le chapitre suivant décrit le contexte organisationnel de l'autorité Gouvernementale de Certification Électronique à partir des données issues de divers documents et des informations glanées auprès de l'organe lui-même. En plus, Il comprend également un cadre méthodologique comprenant l'études qualitatives, ainsi que des informations sur les procédures de recherche de cette approche. Nous avons commencé par une présentation générale dans le but de présenter l'organe au sein de laquelle s'est déroulé le sujet de notre étude.

Section 01: Introduction à la recherche qualitative

Il est important de noter que la recherche qualitative englobe toutes les formes d'enquêtes sur le terrain qui se concentrent sur les discours et les descriptions de vie. Cette approche est particulière en ce qu'elle examine les phénomènes sociaux dans leur milieu naturel, et non dans des milieux artificiels ou expérimentaux. Étant liées aux situations de la vie quotidienne, les expériences et les croyances sont moins pertinentes à analyser dans un contexte décontextualisé. Ainsi, les données sont recueillies par l'échange avec les individus dans leur langue maternelle et par l'observation dans leur milieu de vie habituel. (Kirk et Miller, 1986) ou à l'endroit qu'ils préfèrent. De plus, la recherche qualitative fait souvent appel à diverses méthodes qualitatives pour traiter des sujets.

De plus, la recherche qualitative fait souvent appel à diverses méthodes qualitatives pour traiter une même question de recherche de manière variée. Selon Pope et Mays (2006). Le concept de triangulation permet en partie d'expliquer cela, car il consiste à comparer les résultats obtenus à partir de différentes sources d'information. Selon Pope et Mays (1995) et Bloor et Wood (2006). La recherche qualitative est finalement un processus itératif : elle se construit à partir des hypothèses, des suppositions et des théories qui se transforment au fil des différentes étapes de l'enquête.

1.1 Définition générale d'une étude qualitative

L'objectif de la recherche qualitative consiste à créer des idées qui nous permettent de saisir les phénomènes sociaux dans des environnements naturels (au lieu d'être expérimentaux), en mettant l'accent sur les significations, les expériences et les perspectives de tous les participants. » (Mays et Pope, 1995, p. 43).

Pendant notre expérience au sein de l'entreprise, nous avons été confrontés à des données d'une grande richesse et complexité, ce qui nous a conduit à opter pour une méthodologie de recherche qualitative qui s'avère la plus appropriée pour notre sujet.

Campenhoudt, Marquet, & Quivy (2017) définissent la recherche qualitative comme étant «Un ensemble de méthodes d'investigation dont l'objectif est de donner une vision du comportement et des perceptions des individus et d'analyser de manière approfondie leurs opinions sur un sujet spécifique. Elle produit des idées et des hypothèses qui peuvent aider à saisir la perception d'une question par la population cible et permettre de définir ou de

comprendre les différentes options associées à cette question. Un ensemble de méthodes d'investigation dont l'objectif est de donner une vision du comportement et des perceptions des individus et d'analyser de manière approfondie leurs opinions sur un sujet spécifique. Elle produit des idées et des hypothèses qui peuvent aider à saisir la perception d'une question par la population cible et permettre de définir ou de comprendre les différentes options associées à cette question. ».

1.2 Instruments de collecte d'information :

La collecte de données joue un rôle essentiel dans la mise en œuvre de toute recherche. Différents outils d'analyse et de collecte de données sont utilisés dans la démarche qualitative, ce qui implique de toujours se référer à la question et à la nature de la recherche, ainsi qu'aux caractéristiques du terrain. Trois méthodes de collecte de données ont été sélectionnées pour notre étude: la recherche documentaire, l'observation et enfin, l'entretien. Nous avons trouvé ces méthodes les plus pertinentes et les plus appropriées pour répondre aux exigences de notre problématique. Différents mémoires sur des sujets similaires au nôtre (en particulier à l'ENSM) ont employé ces méthodes de collecte de données. (BENSLAMA Nadia 2019).

1.2.1. La recherche documentaire

Cette recherche vise à collecter des informations préalablement disponibles sur un sujet particulier dans le but de le mieux cerner et pouvoir répondre par la suite à la problématique de départ.

« L'étude documentaire (ou observation documentaire ou étude de documents) concerne des objets dont l'observation est indirecte, d'après les traces qu'ils ont laissées. En ce qui concerne la recherche documentaire, elle offre la possibilité de regrouper la documentation importante sur une question à étudier et de disposer du plus grand nombre d'informations pertinentes dans un domaine spécifique au sujet à aborder ».

L'étude documentaire dans notre cas était considérée non pas comme un objectif de recherche mais comme un support précieux pour une exploration profonde du phénomène étudié

1.2.2. L'observation

L'observation est une méthode très répandue dans une étude qualitative. Elle offre au

chercheur la possibilité de collecter des informations verbales et surtout non verbales, en analysant les comportements et les situations.

1.2.3. L'entretien

“L'entretien consiste en des entretiens oraux individuels ou de groupe avec plusieurs personnes sélectionnées avec soin, dans le but d'obtenir des renseignements sur des faits ou des représentations. L'étude de ces données permet de juger de leur pertinence, de leur validité et de leur fiabilité en considération des objectifs du recueil.” (Berrewaerts 2015)

En effet, l'entretien permet de récolter des données sur les avis, l'attitude et les sentiments de la personne interrogée.

Il existe trois types d'entretiens de recherche : l'entretien directif, l'entretien semi-directif et l'entretien non directif (ou libre). Le degré de liberté du chercheur varie d'un type d'entretien à l'autre (Tableau 3).

Tableau 3: les caractéristiques des trois types d'entretiens

Entretien directif	Entretien semi-directif	Entretien non directif (libre)
Structure bien définie.	Questions/thèmes à traiter préalablement connus.	Aucune question pré-écrite.
Demander aux interlocuteurs les mêmes questions, respecter leur ordre et la durée de l'entretien.	Pendant l'entretien, la personne interrogée a la possibilité de poser de nouvelles questions.	Proposer un sujet global sur lequel la personne interrogée exprime son point de vue.
Questionner les personnes dans les mêmes conditions.	Possibilité de rebondir pour obtenir de nouveaux éléments d'information.	Ne pas s'immiscer dans l'explication, à moins de le relancer et d'encourager la personne à aller davantage.

Source : Claude 2019

Un entretien semi-directif est réalisé en utilisant un guide d'entretien. Il est constitué d'une série de questions, réparties en séries.

Les a catégorisées en 4 phases :

- **La phase d'introduction** : a pour objectif de présenter et d'exposer l'objet de l'entretien à la personne interviewée.
- **La phase du début de l'entretien** : a pour but de poser des questions visant à mieux connaître l'interviewer et le mettre dans position de confort.
- **La phase de réponse** : elle concerne la collecte des informations de la part de l'interviewé, tout en le laissant s'exprimer librement.

Section 02: La présentation de l'organe (Autorité Gouvernementale de Certification Electronique)

L'AGCE joue un rôle essentiel et essentiel dans la réalisation de la transition numérique en Algérie, en tant que fournisseur unique de l'identité numérique reconnue et des technologies avancées de sécurisation des échanges numériques, devenant ainsi le tiers de confiance pour les échanges numériques entre les acteurs gouvernementaux et leurs interlocuteurs.

2.1 Historique

La Loi n°15-04 du 11 Rabie Ethani 1436, publiée le 1er février 2015, établit l'Autorité Gouvernementale de Certification Électronique, qui établit les règles générales concernant la signature et la certification électroniques. Le schéma national de certification électronique a été défini par le législateur et son modèle organisationnel est composé de trois (03) Autorités de Certification Électronique, selon les dispositions suivantes :

- Autorité Nationale de Certification Électronique (ANCE) créée auprès du Premier Ministre,
- Autorité Gouvernementale de Certification Électronique (AGCE) créée auprès du Ministre chargé des télécommunications.
- Autorité Économique de Certification Électronique (AECE) confiée à l'Autorité de Régulation de la Poste et des Communications Électronique (ARPCE).

L'Autorité Gouvernementale de Certification Électronique, qui possède la personnalité morale et l'autonomie financière, est une entité administrative. Selon l'article 2 de la loi 15-04, l'Autorité Gouvernementale de Certification Électronique a pour mission de superviser et de contrôler l'activité de certification électronique des tiers de confiance, ainsi que de fournir des services de certification électronique aux intervenants de la branche gouvernementale. : « institutions et administrations publiques, établissements publics tels que définis par la législation en vigueur, institutions nationales autonomes, autorités de

régulation, intervenants dans les échanges interbancaires, ainsi que toute personne ou entité qui de par sa nature ou mission fait partie de la branche gouvernementale. »

Une cellule d'audit et un secrétariat technique soutiennent la Directrice Générale. Le mois de mai 2021 marque une date inoubliable dans l'histoire de la certification électronique en Algérie : l'Autorité Gouvernementale de Certification Electronique (AGCE) reçoit les certificats de conformité aux référentiels WebTrust for CA, WebTrust BR SSL et WebTrust for Code Signing, tant pour son propre compte que pour celui de l'Autorité Nationale de Certification Electronique (ANCE).

Le programme WebTrust offre une garantie basée sur une série de principes et de critères tels que :

- **Conformité** : les méthodes et les procédures utilisées pour fournir des services de confiance respectent les normes et les meilleures pratiques de l'industrie..

- **Gestion de la sécurité** : consiste à mettre en œuvre des politiques de sécurité afin de garantir la sécurité logique et physique du système.

- **Gestion des opérations** : L'ensemble du personnel applique les procédures opérationnelles conformément au standard de la gestion des services informatiques.

- **Gestion de l'accès au système** : Des mesures de sécurité sont mises en place afin de prévenir les accès non autorisés ou inattendus.

- **Continuité des activités** : On coordonne les plans, les responsabilités et les rôles afin d'assurer la disponibilité des systèmes face aux incidents et aux catastrophes.

Cet audit est effectué chaque année pour préserver la renommée internationale.

La mise en place des Autorités Nationale et Gouvernementale de Certification Electronique, qui a débuté en décembre 2018, a été terminée en novembre 2020 et a été récompensée par les sceaux WebTrust en mai 2021. Cela confirme que les services de l'AGCE respectent les référentiels et les normes internationales en la matière.

Entre décembre 2018 et mai 2021, ces équipes ont réussi à réussir cet exploit malgré toutes les difficultés, notamment celles liées au COVID-19. Cette réussite a été rendue possible grâce à leur professionnalisme, leur détermination et leur persévérance.

Pour l'AGCE et l'ANCE, la première étape de la reconnaissance internationale est donc terminée. Elle offre la possibilité de commencer les processus d'intégration auprès des grandes entreprises mondiales telles que Google, Microsoft, Mozilla, etc.

L'Audit WebTrust a nécessité des ressources matérielles, financières et humaines considérables. Un message puissant adressé aux clients de l'AGCE concernant ses principes, ses objectifs et son engagement à offrir des services à la pointe de la technologie.

Depuis le début du projet par l'AGCE en tant que coordonnateur du schéma national de certification électronique, l'AGCE est devenue l'initiateur et le principal acteur du climat de confiance numérique indispensable à la réalisation des projets de numérisation et de transformation numérique visant à développer l'économie numérique en Algérie..

L'AGCE adopte une approche visant à renforcer la confiance dans les transactions électroniques en généralisant les services de signature et de certification électroniques auprès des acteurs de la branche gouvernementale (AGCE).

Effectivement, grâce à son savoir-faire et à ses équipes pluridisciplinaires composées de jeunes diplômés algériens, L'AGCE assure la sécurité des communications en ligne, la gestion de milliers d'identités numériques vérifiées et l'automatisation des procédures d'authentification et de chiffrement. Grâce à ses infrastructures PKI de pointe et à ses solutions d'identités numériques, il est en mesure de suivre et de contrôler l'activité de certification électronique des tiers de confiance, ainsi que de fournir des services de certification électronique aux intervenants de la branche gouvernementale pour les tiers.

2.2 Produites

2.2.1. Certificats Électronique :

Les certificats électroniques de l'AGCE offrent la possibilité d'identifier et d'authentifier une entité physique ou morale, de sécuriser les échanges numériques et de signer électroniquement des documents et des données en toute sécurité.

Nous produisons et émettons ces certificats en respectant notre CPS (Certificate Practice Statement), qui est conforme et vérifié selon la norme mondiale WebTrust for CA pour les autorités de certification publique.

Dans la réalité, l'AGCE propose diverses catégories de certificats électroniques pour les différentes utilisations suivantes :

2.2.1.1. La Signature de documents:

• **Certificats de signature qualifiée** : Les signatures électroniques qualifiées (High Assurance) légales (Loi 15-04) sont utilisées pour générer des documents et des transactions électroniques certifiés.

- ✓ Il est indéniable que le document signé est authentique. Préserve la fiabilité du document en évitant toute modification non autorisée.]
- ✓ Principe de l'absence de répudiation de la signature.]
- ✓ Certificat qui permet d'identifier la personne et son organisation, ainsi que d'autres caractéristiques sélectionnées par l'entreprise.]
- ✓ Une assurance d'identité solide (High Assurance).]
- ✓ La date et l'heure de la signature sont confirmées par un horodatage fiable.]
- ✓ Encryption minimale 2048 (RSA) 256 (ECDSA).]
- ✓ Le certificat a une durée de validité de 36 mois.]
- ✓ L'AGCE peut héberger les clés de signature à distance dans un QSCD CC EAL4+ ou l'utilisateur peut les héberger localement dans des dispositifs cryptographiques FIPS 140-2 de niveau 2.]
- ✓ Service de validation à l'heure actuelle pour vérifier les certificats.

• **Certificats ESeal** : Utilisés afin d'inclure un certificat électronique sur un document fourni par une organisation. Le certificat eSeal peut être utilisé par un système automatique qui applique des cachets électroniques sur des ensembles de documents sans nécessiter d'intervention humaine, en fonction du mode de mise en œuvre.

Preuve indéniable de l'authenticité du document signé.

- ✓ Préserve la fiabilité des documents en évitant toute modification non autorisée.
- ✓ Principe de l'absence de répudiation de la signature.
- ✓ Certificat permettant d'identifier un département, une structure ou l'ensemble de l'organisation.

- ✓ Une assurance d'identité solide (High Assurance).
- ✓ La date et l'heure de la signature sont confirmées par un horodatage fiable.
- ✓ Le certificat a une durée de validité de 36 mois.
- ✓ Encryption minimale 2048 (RSA) 256 (ECDSA).
- ✓ Service de validation à l'heure actuelle pour vérifier les certificats.

2.2.1.2 L'Authentification :

•Certificats d'authentification : Utilisé pour :

- ✓ authentifier les utilisateurs des services en ligne ;
- ✓ signer et chiffrer les e-mails ;
- ✓ renforcer la sécurité de l'authentification en ligne en utilisant l'authentification par certificat et la signature des e-mails, ce qui ajoute une mesure supplémentaire de confirmation de l'identité, supérieure aux mots de passe et aux secrets traditionnels.

Prendre en charge l'authentification mutualisée entre les serveurs et les utilisateurs.

- ✓ S'assure que toutes les applications sensibles peuvent être accédées avec une seule identité.
- ✓ Offre une protection contre les évasions de mots de passe (les clés privées utilisées pour l'authentification restent toujours en présence de l'utilisateur).
- ✓ Offre la possibilité d'accéder à de nouveaux services en utilisant votre identité et votre authentification sécurisés.
- ✓ Méthode de chiffrement minimale 2048 (RSA) 256 (ECDSA).

La durée de validité du certificat est de 36 mois.

- ✓ Service 24/7 de validation pour vérifier les certificats.

2.2.1.3 Les communications sécurisées :

•**Certificats TLS/SSL** : Les certificats sont utilisés pour authentifier les sites web/serveurs et sécuriser les données transmises.

- Approuvé par Webtrust SSL Basline Requisités.
- Certificats SSL de catégorie « Validation Organisationnelle » (OV).
- Hashage SHA256.

- Accepte les wildcards et les domaines multiples. Certificat de reconnaissance d'un département, d'une structure ou de l'ensemble de l'organisation.

- **Certificats VPN :**

Les certificats sont utilisés pour identifier, authentifier ou chiffrer les données de session.

Offre la possibilité d'authentifier les nœuds et les serveurs connectés au réseau privé de votre entreprise.

- Approuvé par Webtrust SSL Baseline Requisités.
- Certificats de niveau « Organisation Validation » (OV).
- Hashage SHA256.
- S'adapte aux wildcards et aux domaines multiples.
- Certificat qui identifie un département, une structure ou l'ensemble de l'organisation.

2.2.2 La signature électronique

L'AGCE offre des signatures électroniques légales à travers divers services et solutions adaptés à diverses situations d'utilisation métier.

Les utilisateurs peuvent bénéficier d'une signature électronique qualifiée qui leur confère le même caractère légal et juridique qu'une signature manuscrite, ce qui facilite la transition numérique des entreprises et des administrations publiques.

Deux solutions sont utilisées pour fournir les signatures électroniques de l'AGCE, en respectant les normes internationales et l'état de l'art actuel, à savoir :

2.2.2.1. La Signature à Distance :

L'aurotité offre la possibilité de signer à distance pour faciliter la mobilité et la flexibilité des utilisateurs lors de la signature de leurs documents. La technologie essentielle du Virtual ID permet cela, et peut être aisément utilisé grâce à la plateforme de collaboration documentaire E-Tawki3, ou intégré en utilisant les API Restful ou un Plugin Windows.

2.2.2.2 La Signature Locale :

Le système de signature traditionnel implique que l'utilisateur conserve les clés de

signature dans un dispositif cryptographique qui garantit un accès sécurisé à l'intérieur de l'entreprise.

2.3 Solution et services :

A/Le Virtual ID : représente l'identité numérique des individus accessible à distance grâce au Service de Signature à distance offert par l'aurotité .

Les clés de signature des utilisateurs liées à leurs certificats électroniques sont créées de manière sécurisée et stockées sur l'infrastructure de l'aurotité dans un système QSCD certifié

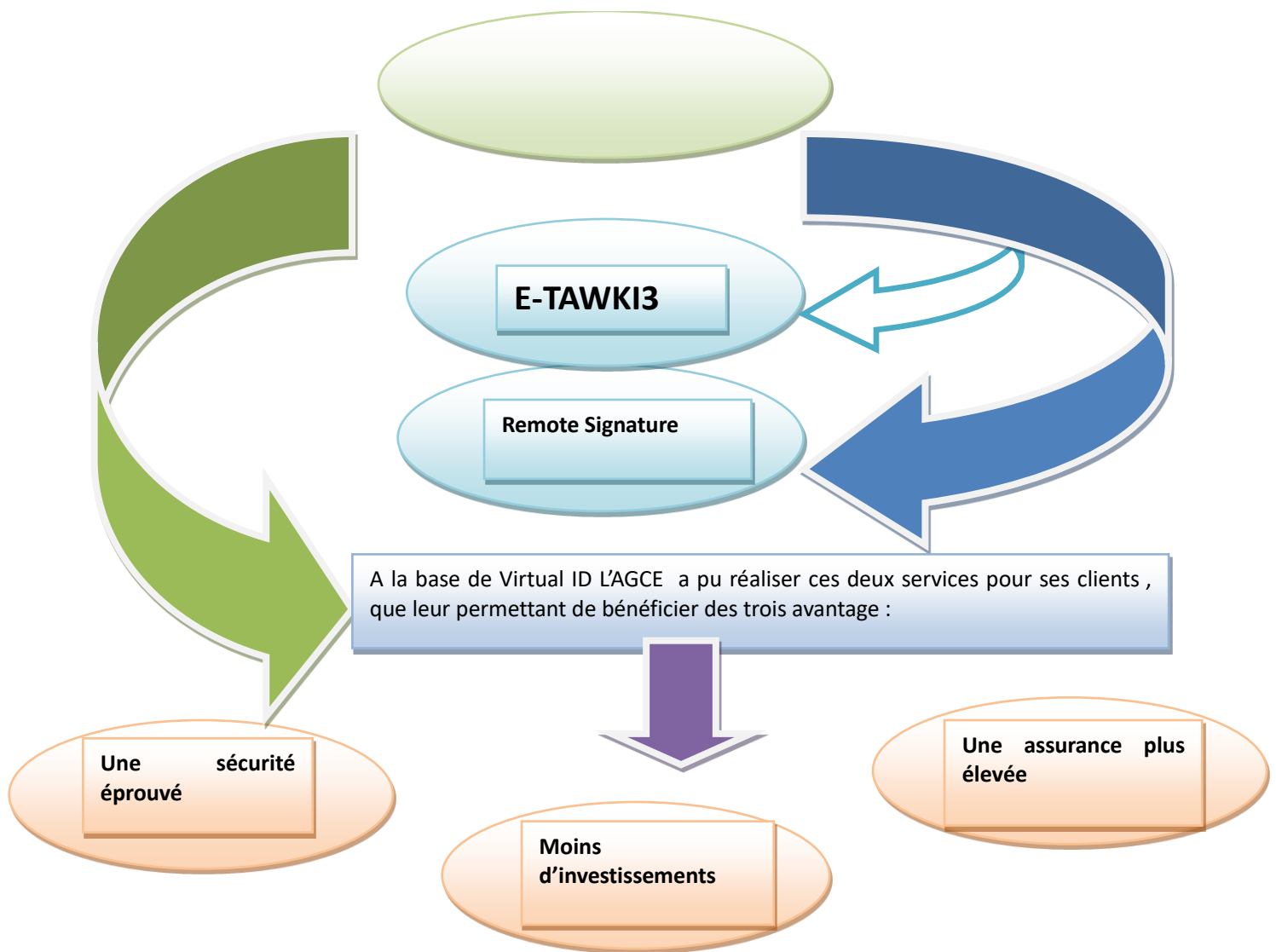
Le profil Certificat de Signature Qualifié est utilisé pour créer le Virtual ID, ce qui autorise la signature de documents avec le Virtual ID. (Loi 15-04)

La technologie du Virtual ID offre une utilisation illimitée, l'aurotité offre différentes options d'implémentation, comme l'intégration du Virtual ID avec E-Tawki3 afin de permettre des signatures électroniques à distance sur la plateforme.

Une application métier spécifique contrôlée par le Client utilise le Virtual ID, qui est connecté au Service de Signature à Distance de l'aurotité.

Le Virtual ID représente la nouvelle génération de l'identité numérique, qui met l'accent sur la mobilité, offrant ainsi un avantage considérable par rapport aux versions traditionnelles des certificats électroniques.

Le Virtual ID offre aux applications et aux services numériques de nouvelles opportunités pour mettre en place la sécurité la plus élevée basée sur la PKI, que ce soit pour la signature de fichiers et de documents, ou pour l'authentification à distance en toute sécurité.



Élaboré par nous même

B/Web RA (Gestion Décentralisée des Certificats Electroniques)

Une structure solide a été établie par l'autorité afin de simplifier l'émission et la distribution de certificats électroniques. Cette mise en place est effectuée en utilisant la force de notre solution WebRA et les méthodes les plus réputées dans le domaine.

- La solution Web RA est constituée de :

- **Autorités Locales d'Enregistrement**

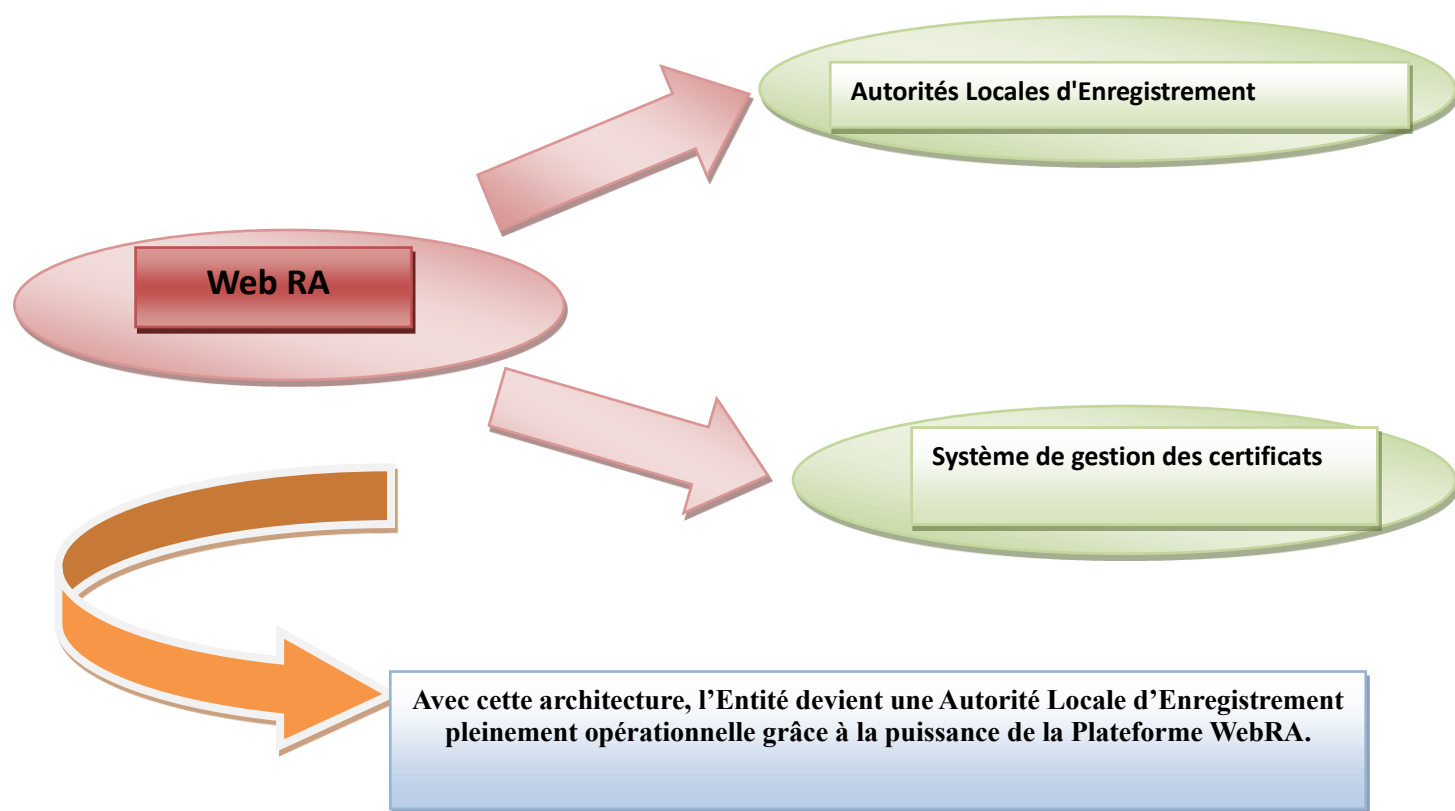
Chaque demande de certificats électroniques est vérifiée et approuvée pour garantir une assurance d'identité optimale et fournir une garantie maximale que l'identité virtuelle est liée à la personne ou à l'entité réelle. L'organisation correspondante à laquelle appartient la personne physique est responsable de la gestion du processus d'authentification des demandes de certificats. Les entreprises profitent donc d'une souplesse dans la gestion des certificats de leurs individus et d'une possibilité d'évolution sans limite.

- **Système de gestion des certificats WebRA**

WebRA offre aux organisations la possibilité de demander, d'émettre et de gérer des certificats électroniques de manière sécurisée grâce à :

- Une interface web facile à utiliser pour les administrateurs (Officiers) et les utilisateurs finaux.
- Accès à nos CA publiques et reconnues.
- Un tableau de bord pour superviser les certificats et gérer les intégrations avec E-Tawki3 et d'autres produits.
- Une PKI à distance (SaaS) disponible 24/7*

Figure 3: schématisation de Web RA de l'AGCE .



Élaboré par nous même

C/ Service de signature à distance de l'AGCE (AGCE Remote Signing Service) :

Le Service de Validation à distance l'autorité propose des fonctionnalités de signature électronique qui permettent aux utilisateurs de signer leurs documents électroniques sur leurs applications bureautiques ou leurs applications métiers à partir de leurs ordinateurs/laptops ou smartphones en utilisant le Virtual ID.

✓ Scénarios d'intégration possibles :

1.API de signature à distance :

L'API de signature à distance de l'autorité est accessible à toute application métier, permettant ainsi l'application de signatures électroniques qualifiées directement à partir de l'interface utilisateur de l'application métier.

2.Plug-in de signature à distance

Le service de signature à distance de l'autorité est accessible aux applications bureautiques en utilisant le plugin de signature à distance, installé sur Windows OS.

D/AGCE Authorization App :

L'application d'autorisation AGCE est un élément essentiel du processus de signature à distance qualifiée. Elle joue un rôle supplémentaire dans l'authentification et sert à obtenir le consentement et l'approbation de l'utilisateur, en utilisant son Virtual ID.

Après avoir reçu une notification sur son application mobile, le signataire est tenu d'approuver toutes les opérations de signature effectuées avec son Virtual ID. On procède à l'autorisation à distance depuis son appareil mobile en utilisant un Protocole de sécurité spécifique.

E/Service d'Horodatage de Confiance :

L'Autorité d'Horodatage AGCE Timestamping Authority (AGCE TSA-DZ) offre une preuve de temps légale, indépendante et incontestable, démontrant que les transactions ont eu lieu à un moment précis, que les documents électroniques ont existé à un moment précis et qu'ils n'ont pas été modifiés par la suite.

L'horodatage peut servir à différents documents électroniques, dans le but de:

- Dater une signature électronique.
- Démontrer la date de réception ou d'émission d'un fichier par courrier électronique.
- Prendre des dates pour des œuvres intellectuelles.
- Sceller des documents numériquement avant leur archivage.
- Veiller à ce que les documents ne soient pas altérés et qu'ils soient intacts.

- Faire respecter les délais établis par la réglementation et fournir des accusés de réception valables.
- Vérifier la date des documents contractuels, tels que les Conditions Générales d'Utilisation et de Vente, ainsi que les documents de Non-Confidentialité.
- Démontrer la réalisation des opérations en ligne.

Ce service est inclut par défaut dans la prestation du Service de Signature à Distance.

F/Service de Validation

Un Service de Validation des identités est mis en place par l'aurotité afin de fournir aux parties qui souhaitent vérifier la validité d'une identité délivrée par l'aurotité l'état des certificats électroniques.

- Les services CRL publient régulièrement en ligne les informations concernant la validité de tous les certificats émis par l'aurotité.
- Le répondeur OCSP a la possibilité de donner un statut de révocation et de validité à toute identité nécessaire.
- L'identification est vérifiée de manière universelle à partir de toute application compatible et sans nécessiter d'authentification.
- Les prestations en ligne OCSP/CRL sont accessibles à l'échelle mondiale en permanence.
- Il est possible d'intégrer la confiance de manière manuelle (en intégrant le certificat de l'Autorité) ou automatiquement (en fonction des mises à jour du magasin de confiance de l'application utilisée).

G/Service de Vérification des Signatures

Le Service de Vérification de Signature de l'aurotité offre une solution hautement fiable et très efficace pour vérifier les documents et les données signés électroniquement. Il peut également valider les certificats d'utilisateurs finaux et toute la chaîne de certificats, y compris la vérification que le certificat n'a pas expiré, n'est pas révoqué, est signé par une autorité de certification de confiance, etc.)

Les signatures de base existantes peuvent être améliorées grâce au Service de

Vérification, qui permet de les convertir en signatures plus avancées. Il est nécessaire d'inclure dans la signature les données de révocation du certificat du signataire ainsi qu'un horaire conforme à la norme RFC. Cela transforme la signature de base du document en une signature vérifiable à long terme, ce qui implique que toutes les informations nécessaires pour vérifier la signature électronique sont intégrées dans le fichier signé et garantissent qu'elle pourra être utilisée dans le futur.

Ce service est inclus par défaut dans la prestation du Service de Signature à Distance

CHAPITRE III: RESULTATS ET DISSCUSSION

Ce troisième et dernier chapitre a pour objectif de présenter, dans un premier temps, l'entretien ainsi que le projet relatif à l'étude de l'identité numérique. Ensuite, nous aborderons les mécanismes de gouvernance en place. Enfin, ce chapitre se conclura par une discussion des résultats obtenus, accompagnée de propositions d'améliorations et de recommandations.

Section 01: Analyse et discussion des resultats

1.1Présentation d’entretien

Notre étude s'inscrit dans une approche de recherche qualitative et, comme mentionné ci-dessus, notre sujet est vaste et nécessite donc une communication directe et une communication directe avec les parties prenantes pour adapter et répondre aux résultats détaillés. Utilisez les informations obtenues lors des observations de pour éviter de tomber dans les généralisations. À cette fin, nous avons élaboré un guide d’entretien semi-directif composé de trois axes et chaque axe contenant plusieurs questions. Les thèmes principaux de ce guide d’entretien sont présentés dans le tableau suivant :

Tableau 4: *Tableau d'Axe d'Entretien*

Thème	Categories d’analyse
E-gouvernance	Gouvernance, secteur, processus, systèmes, interopérabilité, plateformes.
Identité Numérique et E-gouvernance	Identité, carte numérique, sécurité, authentification, certificats, citoyen, personne, accès
Bonnes Pratiques et Normes	Loi, réglementation, normes, certification, sécurité, numériser, numérisation, plateforme, objectifs, indicateurs, management

Source: Elaboré par nos soins

1.2Analyse des résultats

Le tableau d'Axe d'Entretien proposé est structuré en trois grands thèmes, chacun regroupant des catégories d'analyse pertinentes pour l'étude de l'identité numérique et de l'e-

gouvernance. Voici une analyse détaillée de chaque thème et de ses catégories associées :

1.2.1 E-gouvernance

Les fondements de l'e-gouvernance en mettant l'accent sur la gouvernance des processus numériques, les systèmes en place, et l'interopérabilité entre différents secteurs et plateformes.

- L'interopérabilité est un élément clé pour garantir que les systèmes divers peuvent fonctionner ensemble de manière cohérente et sécurisée. Cela inclut la capacité des plateformes numériques à échanger des informations sans entrave.
- Les processus et systèmes analysés ici sont cruciaux pour comprendre comment l'e-gouvernance est structurée et gérée, ainsi que pour identifier les points d'amélioration potentiels.

1.2.2 Identité Numérique et E-gouvernance

Les aspects de l'identité numérique, qui est essentielle à la mise en œuvre efficace de l'e-gouvernance.

- Les termes comme "sécurité", "authentification", et "certificats" sont particulièrement importants car ils se réfèrent aux mécanismes qui garantissent que l'identité numérique est protégée et utilisée de manière appropriée.
- La relation entre le citoyen (ou la personne) et l'accès aux services numériques est également une composante majeure, car elle détermine comment les individus interagissent avec les systèmes d'e-gouvernance.

1.2.3 Bonnes Pratiques et Normes

Le cadre législatif et normatif qui encadre l'identité numérique et l'e-gouvernance.

- Les lois et réglementations établissent les règles du jeu, tandis que les normes et certifications assurent que les systèmes et pratiques sont conformes aux exigences en matière de sécurité et de qualité.
- La numérisation et les plateformes sont au cœur de la transformation digitale, et les objectifs et indicateurs sont essentiels pour mesurer l'efficacité des initiatives en cours.
- Le management est également une catégorie critique, car il concerne la gestion globale de l'identité numérique et des processus d'e-gouvernance.

1.3 Discussion des résultats

1.3.1 Cohérence Thématique

Les thèmes identifiés dans le tableau sont bien alignés avec les enjeux contemporains de l'e-gouvernance et de l'identité numérique. Chaque thème couvre des dimensions essentielles qui doivent être abordées pour une mise en œuvre efficace de l'identité numérique au sein des structures gouvernementales.

1.3.1.1 Complémentarité des Catégories :

Les catégories d'analyse au sein de chaque thème se complètent bien. Par exemple, dans le thème "E-gouvernance", l'accent mis sur les processus et l'interopérabilité suggère une approche holistique qui prend en compte non seulement la technologie mais aussi l'organisation et la gestion des processus. Dans "Identité Numérique et E-gouvernance", les catégories liées à la sécurité et à l'authentification montrent une compréhension approfondie des enjeux techniques et de sécurité inhérents à l'identité numérique.

1.3.1.2 Mise en Relation des Thèmes :

Les thèmes sont interconnectés de manière à offrir une vue d'ensemble complète de l'identité numérique dans le contexte de l'e-gouvernance. Par exemple, les bonnes pratiques et normes légales influencent directement la manière dont l'e-gouvernance et l'identité numérique sont mises en œuvre et gérées, ce qui, à son tour, impacte l'accès et la sécurité pour les citoyens.

1.3.1.3 Implications pour la Recherche

Cette structuration en thèmes et catégories donne une base solide pour l'analyse qualitative dans votre PFE. Elle nous permet de cibler vos entretiens et notre analyse sur des aspects clés, tout en vous donnant la flexibilité d'explorer comment ces aspects interagissent dans la pratique.

Section 02: Recommandation

Suite à l'analyse détaillée des thèmes et catégories de l'entretien sur l'e-gouvernance et l'identité numérique, voici des recommandations pour améliorer la gouvernance numérique et la gestion de l'identité numérique :

2.1 Renforcement de l'Interopérabilité des Systèmes

2.1.1 Recommandation :

Développer des standards ouverts et favoriser l'intégration des systèmes pour améliorer l'interopérabilité entre les différentes plateformes de gouvernance électronique. Cela permettrait une communication fluide entre les différents secteurs et systèmes, rendant les services publics plus efficaces et accessibles.

2.1.2 Justification :

L'analyse montre que l'interopérabilité est un point crucial pour le succès de l'e-gouvernance, en facilitant la coordination intersectorielle et en améliorant l'efficacité des processus.

2.2 Amélioration de la Sécurité et de l'Authentification

2.2.1 Recommandation:

Adopter des méthodes d'authentification plus robustes, telles que l'authentification multi-facteurs (MFA), et renforcer la protection des données personnelles via des mécanismes de cryptage avancés.

2.2.2 Justification :

Le thème de l'identité numérique met en lumière l'importance de la sécurité et de l'authentification pour garantir la confiance des citoyens et protéger leurs informations sensibles.

2.3 Mise en Œuvre d'un Cadre Réglementaire Clair et Uniforme

2.3.1 Recommandation:

Harmoniser les lois, règlements et normes concernant l'identité numérique à travers les différentes juridictions pour créer un cadre légal cohérent qui guide la mise en œuvre de l'e-

gouvernance.

2.3.2 Justification:

La diversité des réglementations peut créer des obstacles à l'efficacité de la gouvernance numérique. Un cadre uniforme permettrait une application plus efficace et une meilleure conformité.

2.4 Sensibilisation et Formation des Utilisateurs

2.4.1 Recommandation :

Lancer des campagnes de sensibilisation pour éduquer les citoyens sur les avantages de l'identité numérique et les former à l'utilisation sécurisée des services de gouvernance électronique.

2.4.2 Justification :

L'acceptation et l'adoption par les utilisateurs sont essentielles pour le succès de l'identité numérique. Une meilleure compréhension par les citoyens réduira les résistances et augmentera l'efficacité des systèmes en place.

2.5 Évaluation Continue et Adaptation des Objectifs

2.5.2 Recommandation :

Mettre en place des indicateurs de performance clairs et procéder à des évaluations régulières des systèmes de gouvernance numérique pour s'assurer qu'ils répondent aux besoins évolutifs des citoyens et des institutions.

2.5.3 Justification :

L'analyse met en avant l'importance des objectifs et indicateurs dans le management des initiatives d'e-gouvernance. Une évaluation continue permet d'adapter les stratégies en fonction des résultats obtenus.

2.6 Promotion de l'Innovation et de la Recherche

2.6.1 Recommandation :

Encourager l'innovation en matière de technologies d'identité numérique et financer la recherche pour explorer de nouvelles solutions et pratiques dans ce domaine.

2.6.2 Justification :

Pour rester à la pointe de la technologie et répondre aux défis futurs, il est essentiel de soutenir l'innovation continue et la recherche appliquée dans le domaine de l'identité numérique et de l'e-gouvernance.

Conclusion :

Ce chapitre nous permet d'explorer plus en détail les aspects de l'identité numérique et de la gouvernance électronique, en mettant en évidence les mécanismes de gouvernance actuels ainsi que l'analyse qualitative des entretiens menés actuellement. Les thèmes clés identifiés – gouvernance électronique, identité numérique, bonnes pratiques et normes – semblent interconnectés et nécessaires à la mise en œuvre efficace de l'identité numérique dans les structures gouvernementales.

CONCLUSION GÉNÉRAL

La gouvernance de l'identité numérique est un levier essentiel pour moderniser les services publics et renforcer la relation entre l'État et les citoyens à l'ère du numérique.

En Algérie, le développement d'un système d'identité numérique sécurisé et fiable pourrait transformer fondamentalement l'administration publique, améliorer l'efficacité des services et accroître la transparence et la confiance dans les organisations gouvernementales.

Cette recherche a exploré les différents aspects de la gouvernance de l'identité numérique, en s'appuyant sur une revue de la littérature, des études de cas internationales, et une analyse des particularités algériennes. Elle a mis en évidence les meilleures pratiques, les défis à surmonter, notamment en matière de sécurité et de protection des données, ainsi que les opportunités à saisir pour établir un système d'identité numérique complet et adapté au contexte algérien.

Pour que l'identité numérique serve véritablement de catalyseur de transformation numérique et de bonne gouvernance, il est nécessaire de renforcer la protection des données personnelles, d'assurer une adoption généralisée par les citoyens et de construire une base solide et sûre.

Recommandations

Les recommandations formulées dans cette étude visent à guider les autorités algériennes dans la prise de ces mesures, visant à construire un système d'identité numérique répondant aux besoins de la population, améliorant l'efficacité administrative et renforçant la récente e-gouvernance en Algérie.

- Développer des standards ouverts et favoriser l'intégration des systèmes pour une meilleure communication entre les plateformes de gouvernance électronique.
- Adopter des méthodes d'authentification plus robustes, comme l'authentification multi-facteurs (MFA), et renforcer la protection des données personnelles via des mécanismes de cryptage avancés.
- Harmoniser les lois, règlements et normes sur l'identité numérique pour un cadre légal cohérent, facilitant l'application et la conformité.
- Lancer des campagnes de sensibilisation pour éduquer les citoyens sur les avantages de l'identité numérique et les former à une utilisation sécurisée des services en ligne.

- Mettre en place des indicateurs de performance et procéder à des évaluations régulières des systèmes pour s'assurer qu'ils répondent aux besoins des citoyens et institutions.
- Encourager l'innovation technologique en matière d'identité numérique et financer la recherche pour développer de nouvelles solutions.

Bibliographie

Aubry, M., & Sow, M. S. (2021, avril). La transformation digitale en entreprise. Eyrolles.

Commission Nationale de l'Informatique et des Libertés. (2023). Dossier thématique de l'identité numérique. CNIL.

Le Président de la République. (2015). Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et la certification électroniques. Disponible sur <https://www.arpce.dz/fr/file/i2n3y8> , consulté le 23/06/2024.

Mandil-avocats. (2014). Règlement (UE) n° 910/2014 relatif à l'identification électronique et aux services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (eIDAS). Disponible sur https://mandil-avocats.com/le-reglement-eidas-identification-electronique-et-services-de-confiance/#_ftn5 , consulté 29/05/2024.

OECD. (2003). OECD e-Government Studies: Finland. Disponible sur https://www.oecd-ilibrary.org/governance/oecd-e-government-studies-finland-2003_9789264102613-en) . consulté le 10/05/2024

ResearchGate. Reviewing the impacts of electronic governance in Asia: Bridging the internal divide. Disponible sur https://www.researchgate.net/publication/296787853_Reviewing_the_impacts_of_electronic_governance_in_Asia_Bridging_the_internal_divide . Consulté le 13/05/2024

Supiot, Alain. (2015). La gouvernance par les nombres*. Fayard.

Tadjedinne, B. (2023). *E-gouvernement en Algérie: État des lieux, obstacles et solutions* (1re éd.). Dar el Imam Malek

Administration Numérique Chaire ULaval. L'émergence et les impacts de l'identité numérique dans les secteurs privé et public*. Disponible sur <https://www.administration-numerique.chaire.ulaval.ca/recherches/lemergence-et-les-impacts-de-lidentite-numerique-dans-les-secteurs-prive-et-public>.

SHS.hal. Disponible sur <https://shs.hal.science/halshs-04430701> . Consulté le 30/04/2024

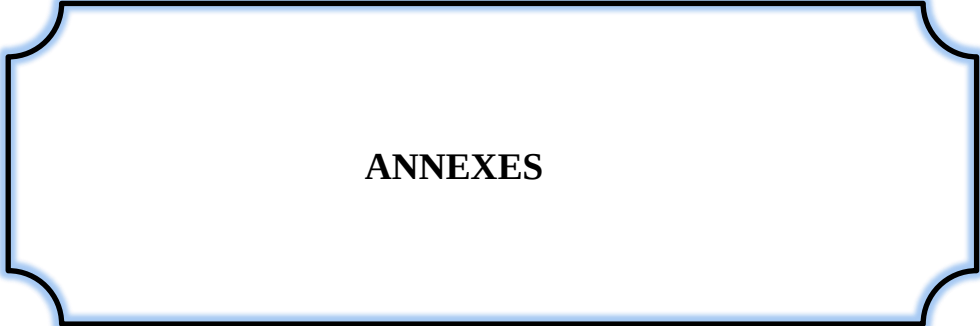
SHS Cairn. 2009. Revue Hermes: La revue. Disponible sur <https://shs.cairn.info/revue-hermes-la-revue-2009-3-page-159?lang=fr> . Consulté le 30/04/2024

SHS Cairn. 2002. Les Cahiers du numérique. Disponible sur <https://shs.cairn.info/revue-les-cahiers-du-numerique-2002-2-page-213?lang=fr> .

OHCHR. About good governance. Disponible sur <https://www.ohchr.org/fr/good-governance/about-good-governance> . Consulté le 20/05/2024

Larousse. Gouvernement. Disponible sur <https://www.larousse.fr/dictionnaires/francais/gouvernement/37698> . consulté le 10/05/2024

Consilium. Data protection régulation. Disponible sur <https://www.consilium.europa.eu/fr/policies/data-protection/data-protection-regulation/> . Consulté le 13/05/2024



ANNEXES

Annexe A : Guide d'entretiens.

Présentation du guide:

Bonjour Mr. /Mme... Nous nous nommons BOUDJEMENE Noumaira et MEDJDOUB Issra, nous sommes étudiantes en 2ème année master, spécialité : Management de l'e-gouvernement à l'Ecole Nationale Supérieure de Management (ENSM). On est en phase finale de préparation de notre projet de fin d'étude. Pour cela, on a besoin de récolter des informations qui nous permettent de traiter la problématique de recherche qui relie les deux concepts clés de notre étude « la e-gouvernance » et « l'identité numérique ».

1. Présentation de l'interviewé :

- Quel poste occupez-vous actuellement ? Dans quelle institution ?
- Pouvez-vous vous présenter brièvement et nous parler de votre parcours professionnel et de vos missions ?

2. Introduction

La e-gouvernance est un objectif stratégique pour l'état qui a de vastes répercussions sur la vie quotidienne des citoyens et un impact positif sur les principaux indicateurs sociétaux. Son étude est importante pour mettre en évidence les exigences et l'impact d'une mise en œuvre réussie. Ce projet vise à mettre en évidence les exigences et les conditions qui conduiraient à une mise en œuvre complète de la e-gouvernance en mettant en valeur le rôle de l'identité numérique.

3. La e-gouvernance :

- Pouvez-vous nous donner une définition de la e-gouvernance ? Qu'est-ce qui distingue l'e-gouvernance de la gouvernance classique ?
- Quel rôle pourra apporter l'e-gouvernement pour les institutions et pour les citoyens ?
- Quelles sont les principales composantes de la e-gouvernance en Algérie ?

4. L'identité numérique et la e-gouvernance :

- Comment définiriez-vous l'identité numérique dans le contexte actuel de la société numérique ?
- Quels sont les formes de l'identité numérique que vous connaissez ? et quels sont ceux qui sont déployés en Algérie ?

- Quel rôle pourra jouer l'identité numérique pour le développement de la e-gouvernance ?

- Quels rôles les autorités et les institutions devraient-elles jouer dans la fourniture et la gestion de l'identité numérique ?

5. **Bonnes pratiques et normes**

- Quelles sont les bonnes pratiques et les normes à mettre en place pour garantir la sécurité et l'intégrité de l'identité numérique ?

- Comment pensez-vous que les normes et les bonnes pratiques devraient être élaborées et appliquées ?

6. **Conclusion**

- A votre avis, quelles seront les conditions et les démarches pour réussir le déploiement de la e-gouvernance avec l'identité numérique en Algérie ?

